User Guide

hp StorageWorks Secure Fabric OS 4.2.x

First Edition (April 2004)

Part Number: AA-RV2EA-TE

This user guide provides procedures for setting up and configuring Secure Fabric OS v4.2.x.

Printed in the U.S.A.

Secure Fabric OS 4.2.x User Guide
First Edition (April 2004)
Part Number: AA-RV2EA-TE

contents

about this guide

This user guide provides information to help you:

- Understand the Secure Fabric OS authentication process
- Add the Secure Fabric OS features to your SAN
- Configure and activate Secure Fabric OS
- Creat Secure Fabric OS policies

“About this Guide” topics include:

Overview

This section covers the following topics:

Intended Audience

This book is intended for use by system administrators and technicians who are experienced with the following:

- HP StorageWorks Fibre Channel SAN switches
- Fabric Operating System version 4.2.x or later

Related Documentation

Documentation, including white papers and best practices documents, is available via the HP website. Please go to:

http://www.hp.com/country/us/eng/prodserv/storage.html

To access Secure Fabric OS v4.2.x related documents:

1. Locate the "Networked storage" section of the web page.
2. Under "Networked storage," go to the "By type" subsection.
3. Click SAN infrastructure. The SAN infrastructure page displays.
4. Locate the Fibre Channel Switches section.
5. Locate the B-Series Fabric subsection, then go to the "Entry-level" subsection.
6. To access version 4.2.x documents (like this document), select SAN Switch 2/8V, SAN Switch 2/16V or SAN Director 2/128.
7. The switch overview page displays.
8. Go to the "product information section," located on the far right side of the web page.
9. Click technical documents.
10. Follow the onscreen instructions to download the applicable documents.

Conventions

Conventions consist of the following:

- Document Conventions
- Text Symbols
- Equipment Symbols

Document Conventions

This document follows the conventions in Table 1.

Table 1: Document conventions

Convention	Element
Blue text: Figure 1	Cross-reference links
Bold	Menu items, buttons, and key, tab, and box names
Italics	Text emphasis and document titles in body text
`Monospace font`	User input, commands, code, file and directory names, and system responses (output and messages)
`Monospace, italic font`	Command-line and code variables
Blue underlined sans serif font text (http://www.hp.com)	Web site addresses

Text Symbols

The following symbols may be found in the text of this guide. They have the following meanings:

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.

Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Tip: Text in a tip provides additional help to readers by providing nonessential or optional techniques, procedures, or shortcuts.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Equipment Symbols

The following equipment symbols may be found on hardware for which this guide pertains. They have the following meanings:

Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of personal injury from electrical shock hazards, do not open this enclosure.

Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of personal injury from a hot component, allow the surface to cool before touching.

Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of personal injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our web site: http://www.hp.com.

HP Technical Support

Telephone numbers for worldwide technical support are listed on the following HP web site: http://www.hp.com/support/. From this web site, select the country of origin.

Note: For continuous quality improvement, calls may be recorded or monitored.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Storage Web Site

The HP web site has the latest information on this product, as well as the latest drivers. Access storage at: http://www.hp.com/country/us/eng/prodserv/storage.html. From this web site, select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP web site for locations and telephone numbers: http://www.hp.com.

Introducing Secure Fabric OS

1

This chapter contains the following sections:

Overview

Secure Fabric OS is an optionally licensed product that provides customizable security restrictions through local and remote management channels on an HP StorageWorks fabric. Secure Fabric OS provides the ability to do the following:

- Create policies to customize fabric management access
- Specify which switches and devices can join the fabric
- View statistics related to attempted policy violations
- Manage the fabric-wide Secure Fabric OS parameters through a single switch
- Create temporary passwords specific to a login account and switch
- Enable and disable Secure Fabric OS as desired

Secure Fabric OS uses digital certificates based on PKI to provide switch-to-switch authentication.

Management Channel Security

Secure Fabric OS can be used to increase the security of the local and remote management channels, including Fabric Manager, Web Tools, standard SNMP applications, Management Server, and a supported Command Line Interface (CLI) client such as *sectelnet*.

The access through a channel can be restricted by customizing the Secure Fabric OS policy for that channel. Secure Fabric OS policies are available for telnet (includes *sectelnet* and Secure Shell), SNMP, Management Server, HTTP, and API.

Fabric Manager, Web Tools, and API all use HTTP and API to access the switch. To use any of these management tools to access a fabric that has Secure Mode enabled, ensure that the workstation computers can access the fabric by both API and HTTP. If an API or HTTP policy has been created, it must include the IP addresses of all workstations.

Note: The **Telnet** button in Web Tools can be used to launch telnet only (not *sectelnet* or Secure Shell) and is disabled when Secure Mode is enabled.

Secure Shell

Fabric OS 4.2.x supports Secure Shell, which is a fully encrypted protocol for CLI. Use of Secure Shell requires installation of a Secure Shell client on the host computer; it does not require a digital certificate on the switch.

Secure Shell access is configurable by the Telnet Policy that is available through Secure Fabric OS. However, Fabric OS v4.2.x supports Secure Shell whether or not Secure Fabric OS is licensed.

To restrict CLI access to Secure Shell over the network, disable telnet as described in "Telnet" on page 18.

Secure Shell clients are available in the public domain and can be located by searching on the Internet. Use clients that support version 2 of the protocol, such as OpenSSH or F-Secure.

Secure Fabric also supports the following ciphers for session encryption and Hash Function-Based Message Authentication Code (HMAC):

- Ciphers: AES128-CBC, 3DES-CBC, Blowfish-CBC, Cast128-CBC, and RC4
- HMACs: HMAC-MD5, HMAC-SHA1, HMAC-SHA1-96, and HMACMD5-96

Note: The first time a Secure Shell client is launched, a message is displayed, indicating that the server's host key is not cached in the registry. You will also see this message the first time a Secure Shell client is launched after you upgrade switch firmware.

For more information about Secure Shell, refer to the *HP StorageWorks Fabric OS 4.2.x Procedures User Guide*.

Sectelnet

The *sectelnet* command is a secure form of telnet that encrypts passwords only. It is available from your switch supplier. Secure Fabric OS 4.2.x includes the *sectelnet* server; the *sectelnet* client must be installed on the workstation computer.

The *sectelnet* command can be used as soon as a digital certificate is installed on the switch. *Sectelnet* access is configurable by the Telnet Policy.

Telnet

Standard telnet is not available when Secure Mode is enabled.

To remove all telnet access to the fabric, disable telnet through the `telnetd` option of the `configure` command. This configure option does not require disabling the switch. For more information about the `configure` command, refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide*.

Switch-to-Switch Authentication Using PKI

Secure Fabric OS uses digital certificates based on Public Key Infrastructure (PKI) and switch World Wide Names (WWNs) to identify the authorized switches, and to prevent the addition of unauthorized switches to the fabric. A PKI certificate installation utility (PKICERT) is provided for generating Certificate Signing Requests (CSRs) and installing digital certificates on switches.

For information about how to use the PKICERT utility, see "Adding Secure Fabric OS to Switches that Require Upgrading" on page 32.

Fabric Configuration Server Switches

Fabric Configuration Server (FCS) switches are one or more switches that are specified as "trusted" switches (switches that are in a physically secure area) for use in managing Secure Fabric OS. These switches should be both electronically and physically secure.

At least one FCS switch must be specified to act as the primary FCS switch, and one or more backup FCS switches are recommended to provide failover ability in case the primary FCS switch fails.

FCS switches are specified by listing their WWNs in a specific policy called the *FCS policy*. The first switch that is listed in this policy and participating in the fabric acts as the primary FCS switch; it distributes the following information to the other switches in the fabric:

- Zoning configuration
- Secure Fabric OS policies
- Fabric password database
- SNMP community strings
- System date and time

Note: The role of the FCS switch is separate from the role of the principal switch, which assigns Domain IDs. The role of the principal switch is not affected by whether Secure Mode is enabled.

When Secure Mode is enabled, only the primary FCS switch can propagate management changes to the fabric. When a new switch joins the fabric, the primary FCS switch verifies the digital certificate. Then it provides the current configuration, overwriting the existing configuration of the new switch.

Because the primary FCS switch distributes the zoning configuration, zoning databases do not merge when new switches join the fabric. Instead, the zoning information on the new switches is overwritten when the primary FCS switch downloads zoning to these switches, if Secure Mode is enabled on all the switches.

For more information about zoning, refer to the *HP StorageWorks Fabric OS 4.2.x Features User Guide*. For more information about merging fabrics, see "Adding Switches and Merging Fabrics with Secure Mode Enabled" on page 121.

The remaining switches listed in the FCS policy act as backup FCS switches. If the primary FCS switch becomes unavailable for any reason, the next switch in the list becomes the primary FCS switch. A minimum of one backup FCS switch is strongly recommended to reduce the possibility of having no primary FCS switch available. You can designate as many backup FCS switches as desired; however, all FCS switches should be physically secure.

Any switches not listed in the FCS policy are defined as non-FCS switches. The root and factory accounts are disabled on non-FCS switches.

Fabric Management Policy Set

Secure Fabric OS supports the creation of several types of policies that can be used to customize various aspects of the fabric. By default, only the FCS policy exists when Secure Mode is first enabled. Secure Fabric OS policies can be created and managed by the CLI or Fabric Manager.

Secure Fabric OS policies can be created, displayed, modified, and deleted. They can also be created and saved without being activated immediately, to allow implementation at a future time. Saved policies are persistent, meaning that they are saved in flash memory and remain available after a switch reboot or power cycle.

The group of existing policies is referred to as the Fabric Management Policy Set (FMPS) which contains an active policy set and a defined policy set. The active policy set contains the policies that are activated and currently in effect. The defined policy set contains all the policies that have been defined, whether activated or not. Both policy sets are distributed to all switches in the fabric by the primary FCS switch. Secure Fabric OS recognizes each type of policy by a predetermined name.

Available Secure Fabric OS Policies

Secure Fabric OS supports the following policies:

- FCS policy—Use to specify the primary FCS and backup FCS switches. This is the only required policy.
- Management Access Control (MAC) policies: Use to restrict management access to switches. The following specific MAC policies are provided:
  - Read and Write SNMP policies—use to restrict which SNMP hosts are allowed read and write access to the fabric.
  - Telnet policy— use to restrict which workstations can use *sectelnet* or Secure Shell to connect to the fabric (telnet is not available when Secure Fabric OS is enabled).
  - HTTP policy—use to restrict which workstations can use HTTP to access the fabric.
  - API policy—use to restrict which workstations can use API to access the fabric.
  - Management Server policy—use to restrict which devices can be accessed by the management server.
  - Serial Port policy—use to restrict which switches can be accessed by serial port.
  - Front Panel policy—use to restrict which switches can be accessed by front panel.
  - Options policy—use to restrict the types of WWNs that can be used for zoning.
- Device Connection Control (DCC) policies—use to restrict which Fibre Channel device ports can connect to which Fibre Channel switch ports.
- Switch Connection Control (SCC) policy—use to restrict which switches can join the fabric.

Adding Secure Fabric OS to the Fabric

2

This chapter contains the following sections:

Overview

Secure Fabric OS is supported by Fabric OS v2.6.1, v3.1.0, and v4.1.0 and higher; it can be added to fabrics that contain any combination of these versions.

However, this guide applies to v2.6.2, v3.1.2 and v4.2.x and assumes these versions are running before upgrading to the latest version of Secure Fabric OS.

The procedure for adding Secure Fabric OS to a switch depends on whether the switch is shipped with one of the above versions installed or requires upgrading.

The following switches will require an upgrade to v4.2.x to use this Secure Fabric OS feature:

- HP StorageWorks SAN Switch 2/32
- HP StorageWorks Core Switch 2/64 switches running Fabric OS v4.x or later

---

Note: The HP StorageWorks SAN Switch 2/8V, HP StorageWorks SAN Switch 2/16V and HP StorageWorks SAN Director 2/128 switches ship with v4.2.x firmware, which fully integrates the Secure Fabric OS feature.

Adding Secure Fabric OS to a Fabric

To add Secure Fabric OS to a fabric, each switch in the fabric must have the following:

- A compatible version of Fabric OS
- An activated Secure Fabric OS license
- An activated Zoning license (zoning is essential to Secure Fabric OS mechanisms)
- The required PKI objects
- A digital certificate

The following tasks are required to set up a fabric for use with Secure Fabric OS:

- Identify the versions of Fabric OS currently installed on each switch, and determine which switches require upgrading to support Secure Fabric OS. Instructions are provided in "Identifying the Current Version of Fabric OS" on page 28.
- For each switch (except Core Switch 2/64) that was shipped with Fabric OS v3.1.2 or v4.2.x installed, follow the instructions provided in "Adding Secure Fabric OS to v3.1.2 or v4.2.x Switches" on page 29.
- For each switch that must be upgraded for use with Secure Fabric OS, follow the instructions provided in "Adding Secure Fabric OS to Switches that Require Upgrading" on page 32.
- For Core Switch 2/64 switches with any version of Fabric OS v4.x, follow the instructions provided in "Adding Secure Fabric OS to an HP StorageWorks Core Switch 2/64" on page 57.
- Install a supported CLI client on each computer workstation that will be used to access the fabric. Instructions are provided in "Installing a Supported CLI Client on a Computer Workstation" on page 60.

Note: If one or more switches are not capable of enforcing the Secure Fabric OS policies, these switches may segment from the fabric.

Identifying the Current Version of Fabric OS

Before continuing, identify the version of Fabric OS on each switch in the fabric, and determine which switches must be upgraded.

To identify the current version of Fabric OS installed on a switch in the fabric:

1. Open a CLI connection (serial or telnet) to the appropriate switch.
2. Log in to the switch as admin. The default password is “password”.
3. Enter the `version` command.

   Example

   Entering the `version` command on a SAN Switch 2/32:

```
SAN Switch 2/32:admin> version
Kernel: 2.4.2
Fabric OS: v4.2
Made on: Fri Jan 3 23:02:08 2003
Flash: Jan 3 18:03:35 2003
BootProm: 4.2.17
switch3900:admin>
```

4. Repeat steps 1 through 3 for each switch in the fabric.

Adding Secure Fabric OS to v3.1.2 or v4.2.x Switches

All switches that are shipped with Fabric OS v3.1.2 or v4.2.x installed already have the required PKI objects and a digital certificate. If a switch no longer has the required PKI objects, refer to for information on recreating the PKI objects. If a switch no longer has the required digital certificate, refer to "Obtaining the Digital Certificate File" on page 42 for information on obtaining digital certificates.

To set up Secure Fabric OS on a switch shipped with Fabric OS v3.1.2 or v4.2.x:

1. Change the account passwords from default values as described in "Customizing the Account Passwords" on page 29.
2. If switches running Fabric OS v2.6.2 or v3.1.2 will be in same fabric as switches running Fabric OS v4.2.x, refer to the *HP StorageWorks Fabric OS 4.2.x Procedures User Guide* for instructions on configuring compatible Port Identifier (PID) modes across the switches.

Note: Changing the PID format causes an update to the DCC policies. If you change the PID format, use the `configdownload` command to create a new backup configuration file. Do not upload the old file.

---

3. Ensure that the switch has activated Secure Fabric OS and Zoning software licenses, as described in "Verifying or Activating the Secure Fabric OS and Zoning Licenses" on page 35.

Customizing the Account Passwords

The user is prompted to customize the account passwords at the first login. The prompts continue to display at each login and the `passwd` command remains disabled until the passwords are changed from the default values. Changing the passwords immediately is recommended.

Note: In addition to customizing the passwords for the user, admin, factory, and root accounts, setting both the boot PROM and recovery passwords is strongly recommended. For instructions on setting these passwords, refer to the *HP StorageWorks Fabric OS 4.2.x Procedures User Guide*.

To change the passwords:

1. Open a CLI connection (serial or telnet) to the switch.
2. Log in to the switch as admin. The default password is *password*. The firmware prompts to change all passwords.
3. Change all the passwords to secure passwords, using 8 to 40 alphanumeric characters for each password, with a different password for each account. The new passwords must be different from the default values.

Note: Record the passwords and store them in a secure place. Recovering passwords can require significant effort and can result in fabric downtime.

Verifying or Activating the Secure Fabric OS and Zoning Licenses

The Secure Fabric OS and Zoning features are part of the Fabric OS and can be activated by entering a corresponding license key, available from the switch supplier. A license must be activated on each switch that will be implementing Secure Fabric OS.

Licenses can be activated through the CLI or through Web Tools. This section provides CLI instructions only. For instructions on activating a license through Web Tools, refer to the *HP StorageWorks Advanced Web Tools 4.2.x User Guide*.

To verify or activate a software license through the CLI:

1. Open a CLI connection (serial or telnet) to the switch.
2. Log in to the switch as admin. The default password is `password`.
3. Enter the `licenseshow` command to determine whether the license is already activated. A list of all the activated licenses is displayed. The Secure Fabric OS license is displayed as `Security license`.

Example

```
switch:admin> licenseshow
 1A1AaAaaaAAAA1a:
     Web license
     Zoning license
    Trunking license
     Security license
switch:admin>
```

4. If the Secure Fabric OS and Zoning licenses are already listed, the features are already available and the remaining steps are not required. If either license is not listed, continue with step 5.
5. Contact your authorized HP Sales Representative to purchase the required license key.
6. After the key is received, enter the following:

   `licenseadd "key"`

   Where *key* is the license key string exactly as provided by the switch supplier; it is case sensitive. You can copy it from the email in which it was provided, directly into the CLI.

   Example

```
switch:admin> licenseadd "aAaaaaAaAaAaAaA"
adding license key "aAaaaaAaAaAaAaA"
switch:admin>
```

7. Enter the `licenseshow` command to verify that the license was successfully activated. If the license is listed, the feature is immediately available (the Secure Fabric OS license is displayed as *Security license*).

Adding Secure Fabric OS to Switches that Require Upgrading

This section applies to the following switches:

- HP StorageWorks SAN Switch 8 or 16 running Fabric OS v2.3 through v2.6.2
- HP StorageWorks SAN Switch 2/8EL or HP StorageWorks SAN Switch 2/16EL running Fabric OS previous to v3.1.2
- HP StorageWorks SAN Switch 2/32 running Fabric OS previous to v4.2.x

To set up Secure Fabric OS on a switch that was not shipped with Fabric OS v3.1.2 or v4.2.x:

1. If switches running Fabric OS v2.6.2 or v3.1.2 will be in same fabric as switches running Fabric OS v4.2.x, refer to the *HP StorageWorks Fabric OS 4.2.x Procedures User Guide* for instructions on configuring compatible PID modes.

Note: Changing the PID format causes an update to the DCC policies. If you change the PID format, use the `configdownload` command to create a new backup configuration file. Do not upload the old file.

---

2. Back up the configuration and upgrade the switch to Fabric OS v2.6.2, v3.1.2, or v4.2.x, as appropriate to the switch, as described in "Upgrading to a Compatible Version of Fabric OS" on page 33.
3. Change the account passwords from the default values, as described in "Customizing the Account Passwords" on page 35.
4. The remaining steps are determined by whether Secure Fabric OS was already in use on the switch:
   - If Secure Fabric OS was already in use on the switch, the upgrade is complete; do not proceed further. To verify the existing policy set, enter the `secpolicyshow` command.
   - If Secure Fabric OS was not already in use on the switch, continue with step 5.
5. Verify or activate the Secure Fabric OS and Zoning licenses, as described in "Verifying or Activating the Secure Fabric OS and Zoning Licenses" on page 35.
6. Download and install the PKICERT utility on the computer workstation, as described in "Installing the PKICERT Utility" on page 35.

7. Create a file containing the certificate signing requests (CSRs) from all the switches that require certificates, as described in "Using the PKICERT Utility" on page 36.
8. Obtain digital certificates from the switch supplier, as described in "Obtaining the Digital Certificate File" on page 42.
9. Distribute the certificates to the switches, as described in "Distributing Digital Certificates to the Switches" on page 43.
10. Verify that digital certificates are installed on all the switches, as described in "Verifying Installation of the Digital Certificates" on page 48.

Upgrading to a Compatible Version of Fabric OS

Secure Fabric OS is supported by Fabric OS v2.6, v2.6.2, v3.1.2, and v4.2.x and can be implemented in fabrics that contain any combination of these versions.

The following switches can be upgraded for use with Secure Fabric OS:

- HP StorageWorks SAN Switch 8 or 16 running Fabric OS v2.3 through v2.6.2
- HP StorageWorks SAN Switch 2/8EL or HP StorageWorks SAN Switch 2/16EL running Fabric OS v3.x through 3.1.2
- HP StorageWorks SAN Switch 2/32 or HP StorageWorks Core Switch 2/64 switches running Fabric OS v4.x though v4.2.x

The HP StorageWorks SAN Switch 2/8V, HP StorageWorks SAN Switch 2/16V, and HP StorageWorks SAN Director 2/128 switches ship with v4.2.x firmware, which fully integrates the Secure Fabric OS feature.

Note: Changing the PID format causes an update to the DCC policies. If you change the PID format, use the `configdownload` command to create a new backup configuration file. Do not upload the old file.

Note: Combinations of switches running Fabric OS v2.6.2 or v3.1.2 and Fabric OS v4.2.x must use compatible PID modes. Refer to the *HP StorageWorks Fabric OS 4.2.x Procedures User Guide* for information about PID modes.

If a switch already has a Secure Fabric OS license (such as a switch running Fabric OS v2.6) and Secure Mode is enabled, the switch can remain in Secure Mode during the firmware upgrade.

To install the required versions of Fabric OS on each switch in the fabric:

1. Obtain the required firmware from the switch provider, according to the type of switch.
2. Open a CLI connection (serial or telnet) to one of the switches in the fabric.
3. Back up the configuration by entering the `configupload` command and completing the prompts. This also backs up the security policies, if the switch is an FCS switch.
4. Log in to the switch as admin. The default password is `password`.
5. Download the firmware to the computer workstation or server.
6. Download the required firmware from the computer to the switch. The download process depends on the *type of switch* and the *management interface*. Refer to the *HP StorageWorks Fabric OS 4.2.x Procedures User Guide* for download instructions specific to the type of switch and management interface.

   If Secure Mode is already enabled on the switch (such as on a 2000-series switch that was running v2.6), Secure Mode can remain enabled during the download to preserve the policies.

   For information about merging fabrics that have Secure Mode enabled, refer to "Adding Switches and Merging Fabrics with Secure Mode Enabled" on page 121.
7. Reboot the switch.

Note: The required PKI objects are automatically generated when the switch is rebooted in the new version of Fabric OS. See "Verifying Installation of the Digital Certificates" on page 48 to verify the existence of the PKI objects.

---

8. Repeat this procedure for each switch in the fabric.

Customizing the Account Passwords

After a new version of Fabric OS is installed, you will be prompted to customize the account passwords at the first login. These prompts display at each login and the `passwd` command remains disabled until the passwords are changed from the default values.

Note: In addition to customizing the passwords for the user, admin, factory, and root accounts, setting the boot PROM and recovery passwords is strongly recommended for Fabric OS v4.2.x (this does not apply to v2.6.2 or v3.1.2). For instructions on setting these passwords, refer to the *HP StorageWorks Fabric OS 4.2.x Procedures User Guide*.

To log in and change the passwords:

1. Open a CLI connection (serial or telnet) to the switch.
2. Log in to the switch as admin. The default password is `password`. The firmware prompts the user to change all passwords.
3. Change all the passwords to secure passwords, using 8 to 40 alphanumeric characters for each password, with a different password for each account. The new passwords must be different from the default values.

Note: Record the passwords and store them in a secure place; recovering passwords can require significant effort and can result in fabric downtime.

Verifying or Activating the Secure Fabric OS and Zoning Licenses

To verify or activate Secure Fabric OS and Zoning licenses, refer to the instructions provided in "Verifying Installation of the Digital Certificates" on page 48.

Installing the PKICERT Utility

The PKI certificate installation utility (PKICERT) version 1.0.5 or later is provided by the switch supplier and is used to generate certificate signing requests (CSRs) and install digital certificates on switches. The utility must be installed on a computer workstation.

To install the PKICERT utility on a Solaris workstation, follow the instructions provided in the PKICERT utility ReadMe file.

To install the PKICERT utility on a PC workstation, perform the following steps:

1. Obtain the PKICERT utility from the switch supplier.
2. Extract all the files from the utility zip file into the same location. The default location is *c:\security*. The utility is installed to a subdirectory named `nt_pki`. For example, *c:\security\nt_pki*.

Using the PKICERT Utility

The PKICERT utility lets you retrieve CSRs from all the switches in the fabric and save them into a CSR file in XML format. PKICERT also lets you create reports, and provides online help.

Note: If the procedure to save CSRs in a file is interrupted by a switch reboot, the CSR file is not generated and the procedure must be repeated. This procedure provides PC-specific examples.

To retrieve the CSR file for the fabric:

1. Open the PKICERT utility. On a PC, double-click `pkicert.exe`.

   The utility prompts for the events log file name.

2. Enter a file name for the events log and press **Enter** or just press **Enter** to accept the default. The log file is automatically created in the same directory as `pkicert.exe`.

   Example

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

All events and errors will be recorded in an event/error log file.
If the file already exists, new event/error information will be
appended to it.

Enter a log file name [or just press Enter to accept the default].

[pki_events.log] => pki_events_fabric1.log
```

   The utility prompts for the desired function.

3. Enter **1** to select CSR retrieval and press **Enter**.

Example

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
FUNCTIONS

1)   Retrieve CSRs from switches & write a CSR file
2)   Install Certificates contained in a Certificate file
3)   Generate a Licensed-Product/Installed-Certificates report
4)   Help using PKI-Cert to get & install certificates
q)   Quit PKI Certificate installation utility

Enter choice> 1
```

The utility prompts for the method of specifying fabric addresses.

4. Enter the desired method for entering the fabric addresses, as described below.

Example

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
Choose a method for providing fabric addresses

1)   Manually enter fabric address
2)   Read addresses from a file (name to be given)
r)   Return to Main menu

Enter choice>
```

To manually enter the fabric address:

a. Enter **1** and press **Enter**. The utility prompts for the IP address or switch name of a switch in the fabric. Only one switch name or IP address is required for each fabric.

b. Enter the IP address or switch name of one of the switches in the fabric and press **Enter**. At least one valid IP address must be entered to continue, and the corresponding switch must be operating and available. When all the IP addresses have been entered, press **Enter** again to end the list. The utility prompts for the username and password for this switch.

c. Enter the username and password, then press **Enter** to continue.

Example

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

Only one address per fabric is needed to get to all switches.
Enter a list of one or more IP or DNS addresses (aliases) you
wish to use (one per line). End the list with an empty item.

1 -->  10.32.142.167
2 -->

Connecting to Fabric(s) ...

Login to fabric 1. principal switch WWN = 10:00:00:60:69:80:46:00

Username: admin
Password:

Logged into fabric 1. principal switch WWN = 10:00:00:60:69:80:46:00

Press Enter to continue >
```

To read the fabric addresses from a file:

a. Enter **2** and press **Enter**. The utility prompts for the path and file name of the file. The addresses in the file must be IP addresses or switch names, each on a separate line.

b. Enter the path and file name of the file that contains the fabric addresses and press **Enter**.

Example

```
Enter the file-name of the Fabric Address file.
File Name ===> \\server\Working\FabricAddresses.txt

Connecting to Fabric(s) ...

Login to fabric 1. principal switch WWN = 10:00:00:60:69:80:46:00
Username:admin
Password:

Logged into fabric 1. principal switch WWN = 10:00:00:60:69:80:46:00

Press Enter to continue >
```

The utility prompts for information about the CSR file to be created.

5. Enter the requested information:
   a. Enter the path and file name for the CSR file to be created; then Enter **y** if the address was entered correctly, or enter **n** and reenter the address, if not.
   b. Enter **y** to include licensed product data in the file. Otherwise, Enter **n**.
   c. Enter **y** to retrieve CSRs from all switches in the fabric or **n** to retrieve CSRs only from switches that do not already have a digital certificate.

Example

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
GET CERTIFICATE SIGNING REQUESTS

You must enter the file-name of the CSR output file to create.
       ------------------------------------------------------
       | Note:                                              |
       |   * The named file will be created                 |
       |   * The file-name may include a directory path     |
       |     that must already exist.                       |
       |   * An extension of '.xml' will be appended to     |
       |     the file name if not already present.          |
       |   * If the file already exists, it will be         |
       |     overwritten.                                   |
        ------------------------------------------------------

File Name ===> test
Is the filename "test.xml" correct? (y/n):  y
**** WARNING, file, "test.sml", already exists!! ****
Do you want to overwrite it <y/n>? > y
Include (optional) licensed product data (y/n)? > y
Get CSRs even from switches with certificates (y/n)? > y
```

Note: If CSRs are retrieved and digital certificates are requested for switches that already have digital certificates, the same digital certificates are provided again. This is not a problem except that retrieving and loading digital certificates in a very large fabric may take a long time.

The utility prompts for which fabrics to retrieve CSRs from.

6. Press **1** to retrieve CSRs only from the fabric identified earlier or **a** to retrieve CSRs from all discovered fabrics; then press **Enter**.

Example

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

Choose a Fabric On Which to Operate

Fabric   World Wide Name          # Switches  Principal
------  ----------------------  ----------  -----------
1)    10:00:00:60:69:80:46:00      34      host1_sw0
a)    All Fabrics
r)    Return to Functions menu

enter your choice> 1
```

The utility displays the success or failure of CSR retrieval.

7. Press **Enter** to continue.

Example

```
        PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

Retrieving CSR's from 1 fabric(s)
1. Got a CSR for Switch: Name="sw_129", IP="10.32.142.129"
2. Got a CSR for Switch: Name="sw_128", IP="10.32.142.128"
3. Got a CSR for Switch: Name="sw_139", IP="10.32.142.139"
4. Got a CSR for Switch: Name="sw_143", IP="10.32.142.143"
5. Got a CSR for Switch: Name="sw_138", IP="10.32.142.138"
6. Got a CSR for Switch: Name="sw_142", IP="10.32.142.142"
7. Got a CSR for Switch: Name="Core_sw0", IP="10.32.142.166"

Wrote 12824 bytes of switch data to file: "\\server\Working\CSR_Fabric1.xml"

Success getting CSRs  & writing them to a CSR file

Press Enter to continue >
```

The **Functions** screen displays.

8. If you are ready to install a digital certificate, select option 2 from the list shown in the following **Functions** screen; do not quit PKICERT.

```
        PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
        FUNCTIONS

1)   Retrieve CSRs from switches & write a CSR file
2)   Install Certificates contained in a Certificate file
3)   Generate a Licensed-Product/Installed-Certificates report
4)   Help using PKI-Cert to get & install certificates
q)   Quit PKI Certificate installation utility

Enter choice> 2
```

The following information displays:

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
Currently Connected Fabrics

Fabric   World Wide Name          # Switches  Principal
------  ----------------------  ----------  -----------
*      10:00:00:60:69:11:f8:f9         15      sec237

_____________________________________________________
       Use Currently Connected Fabrics?

y) Yes, continue with current fabric(s)
n) No, input different Fabric addresses(es)

enter your choice> y
```

After you select **y** (yes), the following information is displayed:

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
LOAD CERTIFICATES

  Enter the file-name of the Certificate input file.
File Name ===> c:/6821.xml

Is the filename "c:/6821.xml" correct? (y/n): y
```

After you select **y** the following information is displayed:

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

Choose a Fabric On Which to Operate

Fabric   World Wide Name          # Switches  Principal
------  ----------------------  ----------  -----------
1)    10:00:00:60:69:11:f8:f9         15      sec237
a)    All Fabrics
r)    Return to Functions menu

enter your choice> 1
```

9. Enter **q** , then **y** to quit the utility.

```
       PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
       FUNCTIONS

1)   Retrieve CSRs from switches & write a CSR file
2)   Install Certificates contained in a Certificate file
3)   Generate a Licensed-Product/Installed-Certificates report
4)   Help using PKI-Cert to get & install certificates
q)   Quit PKI Certificate installation utility

Enter choice> q

QUIT? (y/n) y
```

Obtaining the Digital Certificate File

The switch supplier provides the digital certificates in an XML file that is generated in response to the CSRs. Generally, the digital certificate file is provided by email.

To obtain the digital certificate file, contact the switch supplier and provide the following information:

- The CSR file generated in the previous procedure
- Email address
- Technical contact
- Phone
- Country

The switch supplier provides a confirmation number and the digital certificate file, which contains a certificate for each CSR submitted.

Save the digital certificate file on a secure workstation. The recommended location is in the Secure Fabric OS directory; for example, c:\security\nt_pki\<confirmation number>.xml.

HP recommends that you make a backup copy of the digital certificate file and store it in a secure location.

Distributing Digital Certificates to the Switches

The PKICERT utility can be used to distribute the digital certificates to the switches in the fabric. The utility ensures that each digital certificate is installed on the corresponding switch.

If the utility is run without any task argument, it defaults to interactive mode, in which it prompts for the required input.

Note: If this procedure is interrupted by a switch reboot, the certificate is not loaded and the procedure must be repeated.

To automatically load digital certificates onto one or more switches while retrieving CSRs, go to step 8 in "Using the PKICERT Utility" on page 36.

To manually load digital certificates onto one or more switches:

1. Open the PKICERT utility. On a PC, double-click `pkicert.exe`.

   The utility prompts for the events log file name.

2. Enter a file name for the events log and press **Enter**; alternatively, press **Enter** to accept the default. The log file is automatically created in the same directory as `pkicert.exe`.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

All events and errors will be recorded in an event/error log file.
If the file already exists, new event/error information will be
appended to it.

Enter a log file name [or just press Enter to accept the default].

[pki_events.log] => pki_events_fabric1.log
```

The utility prompts for the desired function.

3. Enter **2** to install the certificates and press **Enter**.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
FUNCTIONS

1)   Retrieve CSRs from switches & write a CSR file
2)   Install Certificates contained in a Certificate file
3)   Generate a Licensed-Product/Installed-Certificates report
4)   Help using PKI-Cert to get & install certificates
q)   Quit PKI Certificate installation utility

Enter choice> 2
```

The utility prompts for the method of specifying fabric addresses.

4. Enter the desired method for entering the fabric addresses.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
Choose a method for providing fabric addresses

1)   Manually enter fabric address
2)   Read addresses from a file (name to be given)
r)   Return to Main menu

Type choice>
```

5. To manually enter the fabric address:
   a. Enter **1** and press **Enter**. The utility prompts for the IP address or switch name of a switch in the fabric. Only one switch name or IP address is required for each fabric.
   b. Enter the IP address or switch name of one of the switches in the fabric and press **Enter**. At least one valid IP address must be entered to continue; the corresponding switch must be operating and available.
   c. When all the IP addresses have been entered, press **Enter** again to end the list. The utility prompts for the username and password for this switch.

d. Enter the username and password; then press **Enter** to continue.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

Only one address per fabric is needed to get to all switches.
Enter a list of one or more IP or DNS addresses (aliases) you
wish to use (one per line). End the list with an empty item.

1 -->  10.32.142.167
2 -->

Connecting to Fabric(s) ...

Login to fabric 1. principal switch WWN = 10:00:00:60:69:80:46:00

Username: admin
Password:

Logged into fabric 1. principal switch WWN = 10:00:00:60:69:80:46:00

Press Enter to continue >
```

6. To read the fabric addresses from a file:
   a. Enter **2** and press **Enter**. The utility prompts for the path and file name of the file. The addresses in the file must be IP addresses or switch names, each on a separate line.
   b. Enter the path and file name of the file that contains the fabric addresses and press **Enter**.

```
Enter the file-name of the Fabric Address file.
File Name ===> \\server\Working\FabricAddresses.txt

Connecting to Fabric(s) ...

Login to fabric 1. principal switch WWN = 10:00:00:60:69:80:46:00
Username:admin
Password:

Logged into fabric 1. principal switch WWN = 10:00:00:60:69:80:46:00

Press Enter to continue >
```

   The utility prompts for the path and file name of the digital certificate file provided by the switch supplier.
7. Enter the path and file name of the digital certificate file and press **Enter**.

If the returned path and file name is correct, Enter **y** and press **Enter**. If not correct, Enter **n**, then retype the path and file name.

```
       PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
LOAD CERTIFICATES

Enter the file-name of the Certificates input file.

File Name ===> \\server\Working\DC_Fabric1.xml
Is the filename "\\server\Working\DC_Fabric1.xml" correct? (y/n):  y
```

The utility prompts for which fabrics to install digital certificates to.

8. Enter **1** to distribute certificates only to the fabric identified earlier or **a** to install certificates to all discovered fabrics; then press **Enter**.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

Choose a Fabric On Which to Operate

Fabric   World Wide Name         # Switches  Principal
------  ----------------------  ----------  -----------
1)    10:00:00:60:69:80:46:00      7          host1_sw0
a)    All Fabrics
r)    Return to Functions menu

enter your choice> 1
```

The new certificates are loaded onto the switches, and the success or fail of each certificate is displayed.

9. Press **Enter** to continue.

```
       PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
Load Certificates onto 1 fabric(s)

1. Loaded Certificate on Switch primaryfcsswitch: WWN-10:00:00:60:69:11:fc:52
2. Loaded Certificate on Switch backupfcsswitch: WWN-10:00:00:60:69:11:fc:53
3. Loaded Certificate on Switch backupfcsswitch: WWN-10:00:00:60:69:11:fc:54
4. Loaded Certificate on Switch nonfcsswitch: WWN-10:00:00:60:69:11:fc:55
5. Loaded Certificate on Switch nonfcsswitch: WWN-10:00:00:60:69:11:fc:56
6. Loaded Certificate on Switch nonfcsswitch: WWN-10:00:00:60:69:11:fc:57
7. Loaded Certificate on Switch nonfcsswitch: WWN-10:00:00:60:69:11:fc:58

7 Certificates were loaded,
0 Certificate loads failed

Press Enter to Continue.
```

Note: The *sectelnet* command can be used as soon as a digital certificate is installed on the switch.

10. Press **Enter**.

    The **Functions** screen is displayed.

11. Enter **q** to quit the utility; then enter **y** and press **Enter** to verify that you want to quit.

```
       PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
       FUNCTIONS

1)   Retrieve CSRs from switches & write a CSR file
2)   Install Certificates contained in a Certificate file
3)   Generate a Licensed-Product/Installed-Certificates report
4)   Help using PKI-Cert to get & install certificates
q)   Quit PKI Certificate installation utility

Enter choice> q

QUIT? (y/n) y
```

Verifying Installation of the Digital Certificates

The installation of the digital certificates can be verified through the CLI. To verify that digital certificates are installed on all the switches in the fabric:

1. Log in to one of the switches in the fabric as admin.
2. Display the PKI objects:
   - For Fabric OS v4.2.x, enter `pkishow`. If the switch is a Core Switch 2/64, enter this command on both logical switches.
   - For Fabric OS v2.6.2 and v3.1.2, enter `configshow "pki"`.

   The command displays the status of the PKI objects.

Note: "Root Certificate" is an internal PKI object. "Certificate" is the digital certificate..

Displaying PKI objects on Fabric OS v4.2.x:

```
switch:admin> pkishow
Passphrase      : Exist
Private Key     : Exist
CSR             : Exist
Certificate     : Exist
Root Certificate: Exist
switch:admin>
```

Displaying PKI objects on Fabric OS v3.1.2:

```
switch:admin> configshow "pki"
Passphrase      : Exist
Private Key     : Exist
CSR             : Exist
Certificate     : Exist
Root Certificate: Exist
switch:admin>
```

3. Verify that `Certificate` shows `Exist`.

   If the certificate shows `Empty` but the other objects show *Exist*, repeat the procedure provided in "Distributing Digital Certificates to the Switches" on page 43.

If any of the other objects show `Empty` or the command displays an error message, re-create the objects as described in "Re-creating PKI Objects if Required" on page 49.

4. Repeat for the remaining switches in the fabric.

Re-creating PKI Objects if Required

The PKI objects (except for the digital certificate) are automatically generated the first time when the firmware is booted. If any of the PKI objects appears to be missing, the switch segments from the fabric.

The PKI objects on Fabric OS v2.6.2, v3.1.2, and v4.2.x can be regenerated by rebooting the switch.

The PKI objects on Fabric OS v4.2.x can also be regenerated through the following procedure.

Note: Secure Mode must be disabled to perform this procedure.

To use the CLI to re-create the PKI objects on Fabric OS v4.2.x:

1. Log in to the switch as admin.
2. Enter the `pkiremove` command. If the switch is a Core Switch 2/64, enter this command on both logical switches.
3. Enter the `pkicreate` command to create new PKI objects. New PKI objects are created without digital certificates. If the switch is a Core Switch 2/64, enter this command on both logical switches. The `pkicreate` command does not work if Secure Mode is already enabled.
4. Enter the `pkishow` command. If the switch is a Core Switch 2/64, enter this command on both logical switches.

   The command displays the status of the PKI objects.

Re-creating PKI objects on Fabric OS v4.2.x:

```
switch:admin> pkicreate
Installing Private Key and Csr...
Switch key pair and CSR generated...
Installing Root Certificate...
switch:admin>
switch:admin> pkishow
Passphrase      : Exist
Private Key     : Exist
CSR             : Exist
Certificate     : Empty
Root Certificate: Exist
switch:admin>
```

5. Repeat for any other switches, as required.
6. If the switch was segmented from the fabric, log in to the switch and enter the `switchdisable` and `switchenable` commands.

Creating PKI Certificate Reports

PKI certificate reports provide information about the number of licenses and switches enabled on your secured fabric. The reports can also be used to audit the fabric.

1. To create a PKI report, select option **3** (shown in the following example), and follow the screen prompts.

   Example

```
        PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
        FUNCTIONS

1)   Retrieve CSRs from switches & write a CSR file
2)   Install Certificates contained in a Certificate file
3)   Generate a Licensed-Product/Installed-Certificates report
4)   Help using PKI-Cert to get & install certificates
q)   Quit PKI Certificate installation utility

Enter choice> 3
```

2. Enter the desired method for entering the fabric addresses.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
Choose a method for providing fabric addresses

1)   Manually enter fabric address
2)   Read addresses from a file (name to be given)
r)   Return to Main menu

Enter choice> 1
```

To manually enter the fabric address:

a. Enter **1** and press **Enter**.

The utility prompts for the IP address or switch name of a switch in the fabric. Only one switch name or IP address is required for each fabric.

b. Enter the IP address or switch name of one of the switches in the fabric and press **Enter**.

c. At least one valid IP address must be entered to continue, and the corresponding switch must be operating and available. When all the IP addresses have been entered, press **Enter** again to end the list. The utility prompts for the username and password for this switch.

d. Enter the username and password; then press **Enter** to continue.

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

Only one address per fabric is needed to get to all switches.
Enter a list of one or more IP or DNS addresses (aliases) you
wish to use (one per line). End the list with an empty item.

1 -->  192.168.156.73_
```

After you enter the IP address or name, the utility logs in to the fabric.

```
Connecting to Fabric(s) ...

Login to fabric 1. principal switch WWN = 10:00:00:60:69:50:0d:9f

Username: root
Password:

Logged into fabric 1. principal switch WWN = 10:00:00:60:69:50:0d:9f

Press Enter to continue >
```

The utility prompts for information about the report file to be created.

3. Enter the requested information:
   a. Enter the path and file name for the report file to be created. Then, enter **y** if the address was entered correctly; if not, enter **n** and reenter the address.
   b. Enter **y** to include licensed product data in the file; otherwise, enter **n**.
   c. Enter **y** to retrieve reports from all switches in the fabric, or enter **n** to retrieve reports only from switches that do not already have a digital certificate.

Example

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
CREATE REPORT ON LICENSED PRODUCTS

You must enter the file-name of the report file to write.

       _____________________________________________________
       | Note:                                             |
       |   * The named file will be created                |
       |   * The file-name may include a directory path    |
       |     that must already exist.                      |
       |   * An extension of '.xml' will be appended to    |
       |     the file name if not already present.         |
       |   * If the file already exists, it will be        |
       |     overwritten.                                  |
        -----------------------------------------------------

File Name ===> SFOS_FAB
Is the filename "SFOS_FAB.xml" correct? (y/n):  y
```

The utility prompts for which fabrics to write reports to.

4. Enter **1** to write certificate reports only to the fabric identified earlier, or **a** to write certificate reports to all discovered fabrics. Press **Enter**.

Example

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

Choose a Fabric On Which to Operate

Fabric   World Wide Name         # Switches  Principal
------  ----------------------  ----------  -----------
1)    10:00:00:60:69:50:0d:9f         2       sec_edge_2
a)    All Fabrics
r)    Return to Functions menu

enter your choice> 1
```

Example

```
PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5

Reporting on Licensed Products of these Fabrics:

Fabric   World Wide Name         # Switches  Principal
------  ----------------------  ----------  -----------
1>      10:00:00:60:69:50:0d:9f      2      sec_edge_2

Wrote 545 bytes of Lic Prod info to file: "SFOS_FAB.xml"
Success compiling and writing license report.
Press enter to continue.
```

5. Press **Enter**.

   The **Functions** screen is displayed.

6. Enter **q** to quit the utility; then enter **y** and press **Enter** to verify you want to quit.

Example

```
       PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
       FUNCTIONS

1)   Retrieve CSRs from switches & write a CSR file
2)   Install Certificates contained in a Certificate file
3)   Generate a Licensed-Product/Installed-Certificates report
4)   Help using PKI-Cert to get & install certificates
q)   Quit PKI Certificate installation utility

Enter choice> q
```

Accessing PKI Certificate Help

The purpose of PKI help is to obtain Command Line Interface (CLI) information about PKICERT and obtain advice on advanced options for power users.

1. To access PKI help, select option **4** (as shown in the following example) and follow the screen prompts.

   Example

```
       PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.5
       FUNCTIONS

1)   Retrieve CSRs from switches & write a CSR file
2)   Install Certificates contained in a Certificate file
3)   Generate a Licensed-Product/Installed-Certificates report
4)   Help using PKI-Cert to get & install certificates
q)   Quit PKI Certificate installation utility

Enter choice> 4
```

Example

```
        HELP USING PKI-CERT TO GET & INSTALL DIGITAL CERTIFICATIONS

        NOTE:This utility will only work with switches running a FAB-OS version
        that supports Fabric Security (e.g. >= v2.6, v3.2, v4.2)

1)   Use PKI-Cert to get CSR's (Certificate Signing Requests) which will be
     written to a data file. The XML format file will contain CSR's for each
     switch (identified by its WWN).

2)   Next, Upload the CSR file to the REVIEWERS --> ? Security Upgrade website. A
data      file will be emailed to you containing a set of digital Certificates,
one for      each switch, in XML format.

3)   Finally, use PKI-Cert to install the Certificates. You will be prompted for
     the name of the data file containing the certificates.

Some options may be given on the command line such as "Log-Level."
Read help for Batch/Command-Line mode usage (y/n)? > y_
```

Example

```
        HELP WITH COMMAND LINE USEAGE OF PKI CERTIFICATE UTILITY

pkicert [-gGil] [_e log-file] [-d data-file] [-a addr-file] [-A switch-addr] [-L
log-level] [-u user-login -p password]

Task Options:
          -g Get CSRs & generate a CSR data file
          -G Get CSRs (even from switches with certificates)
          -i Install Certificates from a data file
          -l Licensed Product Report compile & generate
If none of the above "task" options is given, Pki-Cert will operate in
"Interactive" rather than "Batch" mode.

Other OPtions:

Log-file: -e (events/errors log)
  Path/file-name of log file created and written to (or if it already exists,
  apprended to ) with event/error data
     <Press Enter to Continue> y_
```

Example

```
Data-file: -d
   Path/file-name of input or output file
   * If the task is "Get-CSRs" or "License Rpt", the file is an output file
     created and written to with CSR or License report data.
   * If the task is "Install Certificates", dat is read from it.

Address-file: -a
   Path/file-name of optional input file containing IP addresses or aliases of
fabrics to which sessions should be established. If this argument is not provided,
this data is read from the file indicated by environment variable
'FABRIC_CONFIG_FILE'.

Address--IP: -A
   IP address of switch/fabric with which to connect for the given task.

Log-Level: -L
   Level of information to write to the event log file:
   0 = Silent, 1 = Errors, 2 = Events + Errors, 3 = Debug-info +Events + ...

     <Press Enter to Continue> _
```

2. To end help, press **Enter.**

Example

```
User Login: -u
   User name or account login for switch given with _A option or for use as
   default for all switches given.

Password: -p
   Password must accompany "-u UserLogin" if provided. It must be more than 5
   characters.
        ----- END Of HELP with Batch Usage -----

     <Press Enter to Continue> _
```

Adding Secure Fabric OS to an HP StorageWorks Core Switch 2/64

The two logical switches in Core Switch 2/64 switches require a slightly different procedure from other Fabric OS switches. This procedure applies to all Core Switch 2/64 switches, whether they are shipped with Fabric OS v4.2.x or upgraded to Fabric OS v4.2.x.

Note: Placing the two switches from the same Core Switch 2/64 in separate fabrics is not supported if Secure Mode is enabled on one or both switches.

To set up Secure Fabric OS on a Core Switch 2/64:

Note: The CLI messages from each logical switch might display in both CLI sessions.

---

1. Open a telnet or Secure Shell session to the IP address of either of the logical switches. *Sectelnet* can also be used if the switch was shipped with Fabric OS v4.2.x (and therefore already has a digital certificate).

Note: Fabric OS v4.2.x maintains separate login accounts for each logical switch.

---

2. Enter the `version` command. This shows the firmware version installed on the active CP card.

   If the firmware is Fabric OS v4.0.0c or later, the `firmwareshow` command can be entered for more detailed information about which firmware versions are installed.

Example

```
CoreSwitch2/64:admin> version
Kernel: 2.4.2
Fabric OS: v4.0.2
Made on: Fri Feb 1 23:02:08 2002
Flash: Fri Feb 1 18:03:35 2002
BootProm: 4.2.13b
CoreSwitch2/64:admin>
CoreSwitch2/64:admin> firmwareshow
Local CP (Slot 5, CP0): Active
Primary partition: v4.0.2
Secondary Partition: v4.0.2
Remote CP (Slot 6, CP1): Standby
Primary partition: v4.0.2
Secondary Partition: v4.0.2
CoreSwitch2/64:admin>
```

3. If the firmware version is not Fabric OS v4.2.x or later, back up the configuration and install Fabric OS v4.2.x on both CP cards. For instructions, refer to "Upgrading to a Compatible Version of Fabric OS" on page 33.
4. Log in to one logical switch and change the account passwords from the default values, as described in "Customizing the Account Passwords" on page 35. Then, log in to the other logical switch and change the passwords from the default values.
5. If the logical switches are in separate fabrics, synchronize the fabrics by connecting them to a common external Network Time Protocol (NTP) server.

Note: If the fabric contains any switches running Fabric OS v4.2.x, the server must support a full NTP client. For switches running Fabric OS v2.6.2 or 3.1.2, the server can be SNTP or NTP.

---

   a. Open a telnet or Secure Shell session to either of the logical switches.
   b. Enter `tsclockserver "IP address of NTP server"`.

Note: The IP address can be verified by reentering the command with no operand, which displays the current setting.

---

   c. Repeat for the other logical switch.

Example

```
CoreSwitch2/64switch0:admin> tsclockserver "132.163.135.131"
switch:admin> tsclockserver
132.163.135.131
CoreSwitch2/64switch0:admin>
CoreSwitch2/640:admin>login
login: admin
Password: xxxxxx
CoreSwitch2/64switch1:admin> tsclockserver "132.163.135.131"
CoreSwitch2/64switch1:admin> tsclockserver
132.163.135.131
CoreSwitch2/64switch1:admin>
```

6. Ensure that both logical switches have a Secure Fabric OS license activated, as described in "Verifying Installation of the Digital Certificates" on page 48.

Note: Only one license key is required to enable the same feature on both logical switches.

---

7. Ensure that both logical switches have a Zoning license activated, as described in "Verifying Installation of the Digital Certificates" on page 48.
8. If the firmware was upgraded, perform the following steps:
   a. Download and install the PKICERT utility on the computer workstation, if not already installed, as described in "Installing the PKICERT Utility" on page 35.
   b. Use the PKICERT utility to create a file containing the CSRs of all the switches in the fabric, as described in "Using the PKICERT Utility" on page 36.
   c. Obtain digital certificates from the switch supplier, as described in "Obtaining the Digital Certificate File" on page 42.
   d. Use the PKICERT utility to load the certificates onto both logical switches, as described in "Distributing Digital Certificates to the Switches" on page 43.
   e. Verify that the digital certificates are installed on both logical switches, as described in "Verifying Installation of the Digital Certificates" on page 48. The `pkishow` command referenced in this procedure must be executed from both logical switches.

Installing a Supported CLI Client on a Computer Workstation

Standard telnet sessions work only until Secure Mode is enabled. The following telnet clients are supported after Secure Mode has been enabled:

- *Sectelnet*—*Sectelnet* is a secure form of telnet that is available for switches running Fabric OS v2.6.2, v3.1.2, or v4.2.x. For instructions on installing the *sectelnet* client, see "Installing the Sectelnet Client on a Computer Workstation" on page 61.
- SSH—SSH is a secure form of telnet that is supported only for switches running Fabric OS v4.2.x.You can use SSH clients that use version 2 of the protocol (for example, OpenSSH or F-Secure). Refer to the *HP StorageWorks Fabric OS 4.2.x Procedures User Guide* for client installation instructions.

Accessing Sectelnet from the HP Web Site

Sectelnet is provided on the HP web site:

http://www.hp.com/country/us/eng/prodserv/storage.html

To access:

1. Locate the "Networked storage" section of the web page.
2. Under "Networked storage," go to the "By type" subsection.
3. Click SAN infrastructure. The SAN infrastructure page displays.
4. Locate the Fibre Channel Switches section.
5. Locate the B-Series Fabric subsection, then go to the "Enterprise Class" subsection.
6. Select Core Switch 2/64 & Core Switch 2/64 PowerPak.
7. Select software, firmware & drivers.
8. Select Cross Operating System (BIOS, Firmware, etc.).
9. Select Utility Security.
10. Select Secure Telnet Program for Windows.

Installing the Sectelnet Client on a Computer Workstation

It can be used as soon as a digital certificate is installed on the switch.

To install the *sectelnet* client on a PC workstation:

1. Obtain the PC version of the *sectelnet* file from the switch supplier and copy the file onto the workstation computer.
2. Double-click the zipped file to decompress it.
3. Double-click the `setup.exe` file.
4. Install *sectelnet*`.exe` to a location that is "known" to the computer, such as in the directory containing `telnet.exe`. The location must be defined in the `path` environmental variable. *Sectelnet*.exe is available as soon as setup completes.

To install the *sectelnet* client on a Solaris workstation:

1. Obtain the Solaris version of the *sectelnet* file from the switch supplier and copy the file onto the workstation computer.
2. Decompress the tar file and install it to a location that is "known" to the computer, such as in the directory containing the standard telnet file. The location must be defined in the `path` environmental variable. *Sectelnet* is immediately available.

Creating Secure Fabric OS Policies

3

This chapter contains the following sections:

Overview

The Secure Fabric OS policies make it possible to customize access to the fabric. The FCS policy is the only required policy; all other policies are optional.

Implementing Secure Fabric OS policies requires the following tasks:

- Determining which trusted switches to use as FCS switches to manage Secure Fabric OS. These switches should be in a physically secure area.
- Enabling Secure Mode in the fabric and specifying the trusted switch and one or more backup trusted switches. This automatically creates the FCS policy.
- Determining which additional Secure Fabric OS policies to implement in the fabric; then, creating and activating those policies. An access policy must be created for each management channel that will be used.
- Verifying that the Secure Fabric OS policies are operating as intended. HP recommends that you test a variety of scenarios. For troubleshooting information, see "Troubleshooting" on page 126.

Default Fabric and Switch Accessibility

When Secure Mode is enabled, but no additional Secure Fabric OS policies have been created, fabric and switch access default to the following:

- Switches:
  - Only the primary FCS switch can be used to make Secure Fabric OS changes.
  - Any HP StorageWorks switch can join the fabric, provided it is connected to the fabric and is running Fabric OS 2.6.x or later, 3.1.x or later, or 4.1.x or later
  - All switches in the fabric can be accessed through a serial port.
  - All switches in the fabric that have front panels can be accessed through the front panel.
- Computer hosts and workstations:
  - Any computer can access the fabric by SNMP.
  - Any computer can access any switch in the fabric by using CLI (such as by *sectelnet* or Secure Shell).
  - Any computer can establish an HTTP connection to any switch in the fabric.
  - Any computer can establish an API connection to any switch in the fabric.
- Devices:
  - All devices can access the management server.
  - Any device can connect to any Fibre Channel port in the fabric.
- Zoning: node WWNs can be used for WWN-based zoning.

Enabling Secure Mode

Secure Mode is enabled and disabled on a fabric-wide basis. Secure Mode can be enabled and disabled as often as desired; however, all Secure Fabric OS policies, including the FCS policy, are deleted each time Secure Mode is disabled, and they must be re-created the next time it is enabled. The Secure Fabric OS database can be backed up using the `configupload` command. For more information about this command, refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Manual*.

Secure Mode is enabled using the `secmodeenable` command. This command must be entered through a *sectelnet*, Secure Shell, or serial connection to the switch designated as the primary FCS switch. The command fails if any switch in the fabric is not capable of enforcing Secure Fabric OS policies. If the primary FCS switch fails to participate in the fabric, the role of the primary FCS switch moves to the next available switch listed in the FCS policy.

The `secmodeenable` command performs the following actions:

- Requests the password for the current login.
- Requests new passwords for Secure Mode.
- Creates and activates the FCS policy.
- Distributes the policy set (initially consisting only of FCS policy) to all switches in the fabric.
- Activates and distributes the local zoning configurations.
- Fastboots all switches in the fabric to bring the fabric up in Secure Mode.

No other policies are created except for the FCS policy, and no other Secure Fabric OS-related changes occur to the fabric other than the implementation of the FCS policy.

Note: Other Secure Fabric OS policies can be created after the fastboots are complete.

Caution: Placing the two switches from the same Core Switch 2/64 in separate fabrics is not supported if Secure Mode is enabled on one or both switches.

The following restrictions apply when Secure Mode is enabled:

- Standard telnet cannot be used after Secure Mode is enabled. However, *sectelnet* can be used as soon as a digital certificate is installed on the switch. Secure Shell can be used at any time.
- A number of commands can only be entered from the FCS switches. Refer to "Command Restrictions in Secure Mode" on page 140 for a list of these commands.
- If downloading a configuration to the switch:
  - Download the configuration to the primary FCS switch. A configuration downloaded to a backup FCS switch or non-FCS switch is overwritten by the next fabric-wide update from the primary FCS switch.
  - If the `configdownload` file contains an RSNMP policy, it must also contain a WSNMP policy.
  - The defined policy set in the `configdownload` file must have the following characteristics:
    - The defined policy set must exist.
    - The FCS policy must be the first policy.
    - The FCS policy must have at least one switch in common with the current defined FCS policy in the fabric.
  - The active policy set in the `configdownload` file must have the following characteristics:
    - The active policy set must exist.
    - The FCS policy must be the first policy.
    - The FCS policy must be identical to the active FCS policy in the fabric.

Note: If any part of the configuration download process fails, resolve the source of the problem and repeat the `configdownload` command. For information about troubleshooting the configuration download process, refer to the *HP StorageWorks Fabric OS 4.2.x Procedures User Guide*.

For information about displaying the existing Secure Fabric OS policies, see "Displaying Individual Secure Fabric OS Policies" on page 107.

Note: Enabling Secure Mode fastboots all the switches in the fabric.

To enable Secure Mode in the fabric:

1. Ensure that all switches in the fabric have the following items:
   - Fabric OS v2.6.x, v3.1.x, or v4.1.x or greater
   - An activated Secure Fabric OS license
   - An activated Zoning license
   - Digital certificate
2. Ensure that any zoning configuration downloads have completed on all switches in the fabric. For information specific to zoning, refer to the *HP StorageWorks Fabric OS 4.2.x Features User Guide*.
3. Open a *sectelnet* or Secure Shell connection to the switch that will be the primary FCS switch. The login prompt is displayed.

Note: Most Secure Fabric OS commands must be executed on the primary FCS switch. The `secmodeenable` command must be entered through a *sectelnet* or Secure Shell session.

4. Log in to the switch as admin.
5. Terminate any other *sectelnet* or Secure Shell sessions in the fabric (when using the `secmodeenable` command, no other sessions should be active) and ensure that any other commands entered in the current session have completed.
6. Enter the `secmodeenable` command with no operands to use the command's interactive mode; then, identify each FCS switch at the prompts, (as shown in the next example). Press **Enter** with no data to end the FCS list.

   Alternatively, enter the command followed by the FCS switches:

   ```
   secmodeenable "fcsmember;...;fcsmember"
   ```

   fcsmember is the domain ID, WWN, or switch name of the primary and backup FCS switches, with the primary FCS switch listed first.

Example

Enabling Secure Mode and specifying three FCS switches, one each by domain ID, WWN, and switch name, on Fabric OS v3.1.2 (v4.2.x might differ slightly), using the command's interactive mode:

```
primaryfcs:admin> secmodeenable
This is an interactive session to create a FCS list.

Your use of the certificate-based security features of the software
installed on this equipment is subject to the End User License Agreement
provided with the equipment and the Certification Practices Statement,
which you may review at http://www.switchkeyactivation.com/cps.  By using
these security features, you are consenting to be bound by the  terms of
these  documents.  If you  do not agree to the terms of these documents,
promptly contact the entity from which you obtained this software and do
not use these security features.
Do you agree to these terms?  (yes, y, no, n): [no] y

Current FCS list is empty
Enter WWN, Domain, or switch name(Leave blank when done): 2
Switch WWN is 10:00:00:60:69:11:fc:54

Current FCS list:
  10:00:00:60:69:11:fc:54

Enter WWN, Domain, or switch name(Leave blank when done): 10:00:00:60:69:11:fc:55
Switch WWN is 10:00:00:60:69:11:fc:55

Current FCS list:
  10:00:00:60:69:11:fc:54
  10:00:00:60:69:11:fc:55

Enter WWN, Domain, or switch name(Leave blank when done): HP StorageWorks 24
Switch WWN is 10:00:00:60:69:11:fc:56

Current FCS list:
  10:00:00:60:69:11:fc:54
  10:00:00:60:69:11:fc:55
  10:00:00:60:69:11:fc:56

Enter WWN, Domain, or switch name(Leave blank when done):
Are you done?  (yes, y, no, n): [no] y
Is the FCS correct?  (yes, y, no, n): [no] y
```

The command requests active consent to the terms of the license, requests the identity of the FCS switches, and requests the new passwords required for Secure Mode.

Note: Record the passwords and store them in a secure place; recovering passwords can require significant effort and result in fabric downtime.

7. Enter the following passwords at the prompts, using unique passwords that are different from the default values and contain between 8 to 40 alphanumeric characters:
   - Root password for the FCS switch
   - Factory password for the FCS switch
   - Admin password for the FCS switch
   - User password for the fabric
   - Admin password for the non-FCS switches

Note: The root and factory accounts are disabled on the non-FCS switches. If either of these logins is attempted on a non-FCS switch, an error message is displayed.

Example

Entering passwords after enabling Secure Mode:

```
New FCS switch root password:
Re-enter new password:
New FCS switch factory password:
Re-enter new password:
New FCS switch admin password:
Re-enter new password:
New FCS switch user password:
Re-enter new password:
New Non FCS switch admin password:
Re-enter new password:
Saving passwd...done.
Saving Defined FMPS ...
done
Saving Active FMPS ...
done
Committing configuration...done.
Secure mode is enabled.
Saving passwd...done.
Rebooting...
primaryfcs:admin>
```

All passwords are saved after they are entered. The command distributes the new FCS policy and passwords to all switches in the fabric, activates the local zoning configurations, and fastboots all the switches in the fabric.

Modifying the FCS Policy

Only one FCS policy can exist, and it cannot be empty or deleted if Secure Mode is enabled. The FCS policy is named FCS_POLICY.

Changes made to the FCS policy are saved to permanent memory only after the changes have been saved or activated; they can be aborted later if desired. See "Managing Secure Fabric OS Policies" on page 96

The FCS policy can be modified through any of the following methods:

- Using the `secpolicyfcsmove` command to change the position of a switch in the list, as described in "Changing the Position of a Switch Within the FCS Policy" on page 72.
- Using the `secfcsfailover` command to fail over the primary FCS switch to the next switch in the list, as described in "Failing Over the Primary FCS Switch" on page 73.
- Using the `secpolicyadd` command to add members, as described in "Adding a Member to an Existing Policy" on page 98.
- Using the `secpolicyremove` command to remove members, as described in "Removing a Member from a Policy" on page 99.

Note: If the last FCS switch is removed from the fabric, Secure Mode remains enabled, but no primary FCS switch is available. To specify a new primary FCS switch, enter the `secmodeenable` command again and specify the primary and backup FCS switches. This is the only instance in which the `secmodeenable` command can be entered when Secure Mode is already enabled.

Table 2 lists possible FCS policy states.

Table 2: FCS Policy States

Policy State	Characteristics
No policy, or policy with no entries	Not possible if Secure Mode is enabled.
Policy with one entry	A primary FCS switch is designated but there are no backup FCS switches. If the primary FCS switch becomes unavailable for any reason, the fabric is left without an FCS switch.
Policy with multiple entries	A primary FCS switch and one or more backup FCS switches are designated. If the primary FCS switch becomes unavailable, the next switch in the list becomes the primary FCS switch.

Changing the Position of a Switch Within the FCS Policy

The `secpolicyfcsmove` command can be used to change the order in which switches are listed in the FCS policy. The list order determines which backup FCS switch becomes the primary FCS switch if the current primary FCS switch fails.

To modify the order of FCS switches:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the following:

   ```
   secpolicyshow "Defined", "FCS_POLICY"
   ```

   This displays the WWNs of the current primary FCS switch and backup FCS switch.
3. Enter the `secpolicyfcsmove` command, then provide the current position of the switch in the list and the desired position at the prompts.

   Alternatively, enter `secpolicyfcsmove "`*From, To*`"`

   From is the current position in the list of the FCS switch.

   To is the desired position in the list for this switch.

Example

Moving a backup FCS switch from position 2 to position 3 in the FCS list, using interactive mode:.

```
primaryfcs:admin> secpolicyfcsmove
Pos Primary WWN                    DId     swName.
================================================
1   Yes     10:00:00:60:69:10:02:181       switch5.
2   No      10:00:00:60:69:00:00:5a2       switch60.
3   No      10:00:00:60:69:00:00:133       switch73.
Please enter position you'd like to move from : (1..3) [1] 2
Please enter position you'd like to move to : (1..3) [1] 3

_____________________________________________________
DEFINED POLICY SET
FCS_POLICY
Pos Primary WWN                    DId swName

_____________________________________________________
1   Yes     10:00:00:60:69:10:02:181   switch5.
2   No      10:00:00:60:69:00:00:133   switch73.
3   No      10:00:00:60:69:00:00:5a2   switch60.

_____________________________________________________
primaryfcs:admin>
```

4. Enter the `secpolicyactivate` command.

Failing Over the Primary FCS Switch

The `secfcsfailover` command is used to fail over the role of the primary FCS switch to the backup FCS switch from which the command is entered. This can be used to recover from events such as a lost Ethernet connection to the primary FCS switch.

In addition to failing over the role of the primary FCS switch, this command moves the new primary FCS switch to the top of the list in the FCS policy.

Note: Disabling a switch or removing it from the fabric does not change the order of the FCS policy.

During FCS failover to a backup FCS switch, all transactions in process on the current primary FCS switch are aborted, and any further transactions are blocked until failover is complete.

To fail over the primary FCS switch:

1. If desired, view the current FCS list by logging in as admin to the current primary FCS switch from a *sectelnet* or Secure Shell session and entering the following:

   ```
   secpolicyshow "active","FCS_POLICY"
   ```

   Example

   Entering `secpolicyshow` from the current primary FCS switch, "fcsswitcha".

```
fcsswitcha:admin> secPolicyshow "active","FCS_POLICY"
_____________________________________________________
ACTIVE POLICY SET
FCS_POLICY
Pos Primary WWN                    DId     swName
_____________________________________________________
1   Yes     10:00:00:00:00:00:11:1c1       fcsswitcha
2   No      10:00:00:00:00:00:22:2c2       fcsswitchb
3   No      10:00:00:00:00:00:33:3c3       fcsswitchc
fcsswitcha:admin> logout
```

2. From a *sectelnet* or Secure Shell session, log in as admin to the backup FCS switch to be designated as the new primary FCS switch and enter the `secfcsfailover` command.

Entering `secfcsfailover` from the backup FCS switch “fcsswitchc” and then entering `secpolicyshow`:.

```
fcsswitchc:admin> secfcsfailover
This switch is about to become the primary FCS switch.
All transactions of the current Primary FCS switch will be aborted.
ARE YOU SURE (yes, y, no, n): [no] y
WARNING!!!
The FCS policy of Active and Defined Policy sets have been changed.
Review them before you issue secpolicyactivate again.
fcsswitchc:admin>
fcsswitchc:admin> secpolicyshow "active","FCS_POLICY"
_____________________________________________________
ACTIVE POLICY SET
FCS_POLICY
Pos PrimaryWWN                    DId     swName
_____________________________________________________
1   Yes     10:00:00:00:00:00:33:3c3      fcsswitchc
2   No      10:00:00:00:00:00:11:1c1      fcsswitcha
3   No      10:00:00:00:00:00:22:2c2      fcsswitchb
fcsswitchc:admin>
```

The backup FCS switch becomes the new primary FCS switch, and the FCS policy is modified so that the new and previous primary FCS switches have exchanged places.

Creating Secure Fabric OS Policies Other than the FCS Policy

The FCS policy is automatically created when Secure Mode is enabled; other Secure Fabric OS policies can be created after Secure Mode is enabled. The member list of each policy determines the devices or switches to which the policy applies.

If a policy does not exist, no Secure Fabric OS controls are in effect for that aspect of the fabric. If a policy exists but has no members, that functionality is disabled for all switches in the fabric. As soon as a policy has been created, that functionality becomes disabled for all switches except the members listed in the policy.

Caution: Save policy changes frequently; changes are lost if the switch is rebooted before the changes are saved.

Each supported policy is identified by a specific name, and only one policy of each type can exist (except for DCC policies). The policy names are case sensitive and must be entered in all uppercase. Multiple DCC policies can be created using the naming convention DCC_POLICY_*nnn*, with *nnn* representing a unique string.

Note: HP strongly recommends uploading and saving a copy of the Secure Fabric OS database after creating the desired Secure Fabric OS policies is strongly recommended. The `configupload` command can be used to upload a copy of the configuration file, which contains all the Secure Fabric OS information. For more information about this command, refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Manual*.

Policy members can be specified by device port WWN, switch WWN, domain IDs, or switch WWN, depending on the policy. The valid methods for specifying policy members are listed in Table 3.

Table 3: Valid Methods for Specifying Policy Members

Policy Name	IP Address	Device Port WWN	Switch WWN	Domain IDs	Switch Names
FCS_POLICY	No	No	Yes	Yes	Yes
MAC Policies:	No	No	No	No	No
RSNMP_POLICY	Yes	No	No	No	No
WSNMP_POLICY	Yes	No	No	No	No
TELNET_POLICY	Yes	No	No	No	No
HTTP_POLICY	Yes	No	No	No	No
API_POLICY	Yes	No	No	No	No
MS_POLICY	No	Yes	No	No	No
SERIAL_POLICY	No	No	Yes	Yes	Yes
FRONTPANEL_POLICY	No	No	Yes	Yes	Yes
OPTIONS_POLICY	For information about valid input, see"Creating an Options Policy" on page 89.				
DCC_POLICY_nnn	No	Yes	Yes	Yes	Yes
SCC_POLICY	No	No	Yes	Yes	Yes

Note: If IP addresses are used, 0 is used for an octet indicating that any number can be matched. For example, 192.168.11.0 allows access for al IP devices in the range 192.168.11.0 hrough 192.168.11.255. If domain IDs or switch names are used, the corresponding switches must be in the fabric for the command to succeed.

Creating a MAC Policy

Management Access Control (MAC) policies can be used to restrict the following management access to the fabric:

- Access by hosts using SNMP, telnet/*sectelnet*/Secure Shell, HTTP, API
- Access by device ports using SCSI Enclosure Services (SES) or Management Server
- Access through switch serial ports and front panels

The individual MAC policies and how to create them are described in the following sections. By default, all MAC access is allowed; no MAC policies exist until they are created.

Note: An empty MAC policy blocks all access through that management channel. When creating policies, ensure that all desired members are added to each policy.

Providing fabric access to proxy servers is strongly discouraged. When a proxy server is included in a MAC policy for IP-based management, such as the HTTP_POLICY, all IP packets leaving the proxy server appear to originate from the proxy server. This could result in allowing any hosts that have access to the proxy server to access the fabric.

Read and write SNMP policies can be used to specify which SNMP hosts are allowed read and write access to the fabric. The SNMP hosts must be identified by IP address.

- RSNMP_POLICY (read access)
  Only the specified SNMP hosts can perform read operations to the fabric.
- WSNMP_POLICY (write access)
  Only the specified SNMP hosts can perform write operations to the fabric.

Any host granted write permission by the WSNMP policy is automatically granted read permission by the RSNMP policy.

Note: If an SNMP policy is created, it must contain the primary FCS switch and backup FCS switches. This ensures consistent read/write access to the primary FCS switch, even in the event of a failover.

Table 4 lists the expected read and write behaviors resulting from combinations of the RSNMP and WSNMP policies.

Table 4: Read and Write Behaviors of SNMP Policies

RSNMP Policy	WSNMP Policy	Read Result	Write Result
Nonexistent	Nonexistent	Any host can read	Any host can write
Nonexistent	Empty	Any host can read	No host can write
Nonexistent	Host B in policy	Any host can read	Only B can write
Empty	Nonexistent	This combination is not supported. If the WSNMP policy is not defined, the RSNMP policy cannot be created.	
Empty	Empty	No host can read	No host can write
Empty	Host B in policy	Only B can read	Only B can write
Host A in policy	Nonexistent	This combination is not supported. If the WSNMP policy is not defined, the RSNMP policy cannot be created.	
Host A in policy	Empty	Only A can read	No host can write
Host A in policy	Host B in policy	A and B can read	Only B can write

To create an SNMP policy:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the following:

   `secpolicycreate "policy_name", "member;...;member"`

   Policy name is WSNMP_POLICY or RSNMP_POLICY.

   Member is one or more IP addresses in dot-decimal notation. “0” can be entered in an octet to indicate that any number can be matched in that octet.

Example

Creating an WSNMP and an RSNMP policy to only allow IP addresses that match 192.168.5.0 read and write access to the fabric:.

```
primaryfcs:admin> secpolicycreate "WSNMP_POLICY", "192.168.5.0"
WSNMP_POLICY has been created.
primaryfcs:admin>
primaryfcs:admin> secpolicycreate "RSNMP_POLICY", "192.168.5.0"
RSNMP_POLICY has been created.
primaryfcs:admin>
```

3. To save or activate the new policy, enter either `secpolicysave` or `secpolicyactivate`.

   If neither of these commands is entered, the changes are lost when the session is logged out. For more information about these commands, see "Saving Changes to Secure Fabric OS Policies" on page 97 and "Activating Changes to Secure Fabric OS Policies" on page 98.

Telnet Policy

The Telnet policy can be used to specify which workstations can use *sectelnet* or Secure Shell to connect to the fabric. The policy is named TELNET _POLICY and contains a list of the IP addresses for the trusted workstations (workstations that are in a physically secure area).

When an HP StorageWorks Core Switch 2/64 or SAN Director 2/128 is in Secure Mode, *sectelnet* / SSH sessions cannot be opened to the active CP card. This prevents potential violation of the Telnet policy, since the active CP card can be used to access either of the logical switches on the Core Switch 2/64 or SAN Director 2/128. However, *sectelnet* or SSH sessions can be established to the IP addresses of the logical switches and to the standby CP card, if allowed by the Telnet policy. If the active CP card fails over, any *sectelnet* / SSH sessions to the standby CP card are automatically terminated when the standby CP card becomes the active CP card.

See "Creating a Telnet Policy" on page 81.

Note: Static host IP addresses are required to implement the Telnet policy effectively. Do *not* use DHCP for hosts that are in TELNET_POLICY, because as soon as the IP addresses change, the hosts will no longer be able to access the fabric. Restricting output (such as placing a session on "hold" by use of a command or keyboard shortcut) is not recommended.

This policy pertains to *sectelnet* and Secure Shell. It does not pertain to telnet access, because telnet is not available in Secure Mode. *Sectelnet* can be used as soon as a digital certificate is installed on the switch.

Note: An empty TELNET_POLICY blocks all telnet access. To prevent this, keep one or more members in the Telnet policy. If an empty Telnet policy is absolutely required, leave a meaningful entry in the API, HTTP, or SERIAL policies (or do not create these policies) to ensure that some form of management access is available to the switch.

To restrict CLI access over the network to Secure Shell, disable telnet as described in "Telnet" on page 18.

Table 5 lists Telnet policy states.

Table 5: Telnet Policy States

Policy State	Description
No policy	Any host can connect by *sectelnet* or SSH to the fabric.
Policy with no entries	No host can connect by *sectelnet* or SSH to the fabric.
Policy with entries	Only specified hosts can connect by *sectelnet* or SSH to the fabric.

Creating a Telnet Policy

To create a Telnet policy:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the following:

   ```
   secpolicycreate "policy_name", "member;...;member"
   ```

   Policy_name is TELNET_POLICY.

   Member is one or more IP addresses in dot-decimal notation. "0" can be entered in an octet to indicate that any number can be matched in that octet.
3. To save or activate the new policy, enter either the `secpolicysave` or the `secpolicyactivate` command.

   If neither of these commands are entered, the changes are lost when the session is logged out. For more information about these commands, see "Saving Changes to Secure Fabric OS Policies" on page 97 and "Activating Changes to Secure Fabric OS Policies" on page 98.

Example

Creating a Telnet policy to allow anyone on network 192.168.5.024 to access the fabric through a *sectelnet* or Secure Shell session:

```
primaryfcs:admin> secPolicyCreate "TELNET_POLICY", "192.168.5.0"
TELNET_POLICY has been created.
primaryfcs:admin>
```

HTTP Policy

The HTTP policy can be used to specify which workstations can use HTTP to access the fabric. This is useful for applications that use Internet browsers, such as Web Tools.

The policy is named HTTP_POLICY and contains a list of IP addresses for devices and workstations that are allowed to establish HTTP connections to the switches in the fabric.

Table 6 lists possible HTTP policy states.

Table 6: HTTP Policy States

Policy State	Characteristics
No policy	All hosts can establish an HTTP connection to any switch in the fabric.
Policy with no entries	No host can establish an HTTP connection to any switch in the fabric. **Note:** An empty policy causes the message "The page cannot be displayed" to apear when HTTP access is attempted.
Policy with entries	Only specified hosts can establish an HTTP connection to any switch in the fabric.

To create an HTTP policy:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the following:

   `secpolicycreate "policy_name", "member;...;member"`

   Policy_name is HTTP_POLICY.

   Member is one or more IP addresses in dot-decimal notation. "0" can be entered in an octet to indicate that any number can be matched in that octet.

3. To save or activate the new policy, enter either the `secpolicysave` or the `secpolicyactivate` command.

   If neither of these commands are entered, the changes are lost when the session is logged out. For more information about these commands, see "Saving Changes to Secure Fabric OS Policies" on page 97 and "Activating Changes to Secure Fabric OS Policies" on page 98.

   Example

   Creating an HTTP policy to allow anyone on the network with IP address of 192.168.5.0 (where "0" can be any number) to establish an HTTP connection to any switch in the fabric:.

```
primaryfcs:admin> secPolicyCreate "HTTP_POLICY", "192.168.5.0"
HTTP_POLICY has been created.
primaryfcs:admin>
```

API Policy

The API policy can be used to specify which workstations can use API to access the fabric and which ones can write to the primary FCS switch.

The policy is named API_POLICY and contains a list of the IP addresses that are allowed to establish an API connection to switches in the fabric.

Table 7 lists API policy states.

Table 7: API Policy States

Policy State	Characteristics
No policy	All workstations can establish an API connection to any switch in the fabric.
Policy with no entries	No host can establish an API connection to any switch in the fabric.
Policy with entries	Only specified hosts can establish an API connection to any switch in the fabric, and write operations can only be performed on the primary FCS switch.

Creating an API Policy

To create an API policy:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the following:

   `secpolicycreate "policy_name", "member;...;member"`

   Policy_name is API_POLICY.

   Member is one or more IP addresses in dot-decimal notation. "0" can be entered in an octet to indicate that any number can be matched in that octet.
3. To save or activate the new policy, enter either the `secpolicysave` or the `secpolicyactivate` command.

   If neither of these commands are entered, the changes are lost when the session is logged out. For more information about these commands, see "Saving Changes to Secure Fabric OS Policies" on page 97 and "Activating Changes to Secure Fabric OS Policies" on page 98.

   Example

   Creating an API policy to allow anyone on the network with an IP address of 192.168.5.0 (where "0" can be any number) to establish an API connection to any switch in the fabric:

```
primaryfcs:admin> secPolicyCreate "API_POLICY", "192.168.5.0"
API_POLICY has been created.
primaryfcs:admin>
```

SES Policy

The SES policy can be used to restrict which devices can be managed by SES commands. The policy is named SES_POLICY and contains a list of device port WWNs that are allowed to access SES, and from which SES commands are accepted and acted upon.

If Secure Mode is enabled, the SES client must be directly attached to the primary FCS switch. Then the SES client can be used to manage all the switches in the fabric through the SES product. Refer to the *SES User's Guide* for more information.

The current SES implementation does not support the SES commands **Read Buffer** or **Write Buffer** for remote switches. To direct these commands to a switch that is not the primary FCS switch, designate that switch as the primary FCS switch and attach the SES client directly to it.

Table 8 lists possible SES policy states.

Table 8: SES Policy States

Policy State	Characteristics
No policy	All device ports can access SES.
Policy with no entries	No device port can access SES.
Policy with entries	The specified devices can access SES.

Creating an SES Policy

To create an SES policy:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the following:

   `secpolicycreate "policy_name", "member;...;member"`

   Policy_name is SES_POLICY.

   Member is a device port WWN.
3. To save or activate the new policy, enter either the `secpolicysave` or the `secpolicyactivate` command.

   Example

   Creating an SES_POLICY that allows access through a device that has a WWN of 12:24:45:10:0a:67:00:40:

```
primaryfcs:admin> secPolicyCreate "SES_POLICY", "12:24:45:10:0a:67:00:40"
SES_POLICY has been created.
primaryfcs:admin>
```

MS Policy

The Management Server policy can be used to restrict which devices can be accessed by the Management Server. Fabric configuration and control functions can be performed only by requesters that are directly connected to the primary

FCS switch. The policy is named MS_POLICY and contains a list of device port WWNs for which the management server implementation in Fabric OS (designed according to FC-GS-3 standard) accepts and acts on requests.

Table 9 lists Management Server policy states.

Table 9: MS Policy States

Policy State	Characteristics
No policy	All devices can access the management server.
Policy with no entries	No devices can access the management server.
Policy with entries	Specified devices can access the management server.

Creating a MS Policy

To create a Management Server policy:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the following:

   `secpolicycreate "policy_name", "member;...;member"`

   Policy_name is MS_POLICY.

   Member is a device WWN.
3. To save or activate the new policy, enter either the `secpolicysave` or the `secpolicyactivate` command.

   If either of these commands is not entered, the changes are lost when the session is logged out. For more information about these commands, see "Saving Changes to Secure Fabric OS Policies" on page 97 and "Activating Changes to Secure Fabric OS Policies" on page 98.

Example

Creating an MS_POLICY that allows access through a device that has a WWN of 12:24:45:10:0a:67:00:40:

```
primaryfcs:admin> secPolicyCreate "MS_POLICY", "12:24:45:10:0a:67:00:40"
MS_POLICY has been created.
primaryfcs:admin>
```

Serial Port Policy

The Serial Port policy can be used to restrict which switches can be accessed by serial port. The policy is named SERIAL_POLICY and contains a list of switch WWNs, domain IDs, or switch names for which serial port access is enabled.

The serial policy is checked before the account login is accepted. If the Serial Port Policy exists and the switch is not included in the policy, the session is terminated.

Table 10 lists possible Serial Port policy states.

Table 10: Serial Port Policy States

Policy State	Characteristics
No policy	All serial ports of the switches in the fabric are enabled.
Policy with no entries	All serial ports of the switches in the fabric are disabled.
Policy with entries	Only specified switches can be accessed through the serial ports.

Creating a Serial Port Policy

To create a Serial Port policy:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the following:

   `secpolicycreate "policy_name", "member;...;member"`

   Policy_name is MS_POLICY.

   Member is a device WWN.
3. To save or activate the new policy, enter either the `secpolicysave` or the `secpolicyactivate` command.

   If either of these commands is not entered, the changes are lost when the session is logged out. For more information about these commands, see "Saving Changes to Secure Fabric OS Policies" on page 97 and "Activating Changes to Secure Fabric OS Policies" on page 98.

Example

Creating a SERIAL_POLICY that allows serial port access to a switch that has a WWN of 12:24:45:10:0a:67:00:40:

```
primaryfcs:admin> secPolicyCreate "SERIAL_POLICY", "12:24:45:10:0a:67:00:40"
SERIAL_POLICY has been created.
primaryfcs:admin>
```

Front Panel Policy

The Front Panel policy can be used to restrict which switches can be accessed through the front panel. This policy only applies to HP StorageWorks 1 GB switches, since no other switches contain front panels. The policy is named FRONTPANEL_POLICY and contains a list of switch WWNs, domain IDs, or switch names for which front panel access is enabled.

"Creating a Front Panel Policy" on page 88 lists possible policy states.

Table 11: Front Panel Policy States

Policy State	Characteristics
No policy	All the switches in the fabric have front panel access enabled.
Policy with no entries	All the switches in the fabric have front panel access disabled.
Policy with entries	Only specified switches in the fabric have front panel access enabled.

Creating a Front Panel Policy

To create a Front Panel policy:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the following:

   `secpolicycreate "policy_name", "member;...;member"`

   Policy_name is MS_POLICY.

   Member is a device WWN.
3. To save or activate the new policy, enter either the `secpolicysave` or the `secpolicyactivate` command.

If either of these commands is not entered, the changes are lost when the session is logged out. For more information about these commands, see "Saving Changes to Secure Fabric OS Policies" on page 97 and "Activating Changes to Secure Fabric OS Policies" on page 98.

Example

Creating a Front Panel policy to allow only domains 3 and 4 to use the front panel:

```
primaryfcs:admin> secPolicyCreate "FRONTPANEL_POLICY", "3; 4"
FRONTPANEL_POLICY has been created.
primaryfcs:admin>
```

Creating an Options Policy

The Options policy can be used to prevent the use of node WWNs to add members to zones. This policy is named OPTIONS_POLICY and has only one valid value, **"**NoNodeWWNZoning**".** Adding this value to the policy prevents use of Node WWNs for WWN-based zoning.

The use of node WWNs can introduce ambiguity because the node WWN might also be used for one of the device ports, such as a Host Bus Adapter (HBA). If the policy does not exist or is empty, node WWNs can be used for WWN-based zoning. Only one Options policy can be created. This policy cannot be used to control use of port WWNs for zoning.

By default, use of node WWNs is allowed; the Options policy does not exist until it is created by the administrator.

Table 12 lists possible Options policy states.

Table 12: Options Policy States

Policy State	Characteristics
No policy	Node WWNs can be used for WWN-based zoning.
Policy with no entries	Node WWNs can be used for WWN-based zoning.
Policy with entries	Node WWNs cannot be used for WWN-based zoning.

To create an Options policy:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the following:

   `secpolicycreate "policy_name", "member;...;member"`

   Policy_name is MS_POLICY.

   Member is a device WWN.
3. To save or activate the new policy, enter either the `secpolicysave` or the `secpolicyactivate` command.

If either of these commands is not entered, the changes are lost when the session is logged out. For more information about these commands, see "Saving Changes to Secure Fabric OS Policies" on page 97 and "Activating Changes to Secure Fabric OS Policies" on page 98.

4. To apply the change to current transactions, disable the switch then re-enable it by entering the `switchdisable` and `switchenable` commands. This stops any current traffic between devices that are zoned using node names.

   Example

```
primaryfcs:admin> secPolicyCreate "OPTIONS_POLICY", "NoNodeWWNZoning"
OPTIONS_POLICY has been created.
primaryfcs:admin>
```

Creating a DCC Policy

Multiple DCC policies can be used to restrict which device ports can connect to which switch ports. The devices can be initiators, targets, or intermediate devices such as SCSI routers and loop hubs. By default, all device ports are allowed to connect to all switch ports; no DCC policies exist until they are created by the administrator.

Each device port can be bound to one or more switch ports; the same device ports and switch ports might be listed in multiple DCC policies. After a switch port is specified in a DCC policy, it permits connections only from designated device ports. Device ports that are not specified in any DCC policies are allowed to connect only to switch ports that are not specified in any DCC policies.

Note: Some older private loop HBAs do not respond to port login from the switch and are not enforced by the DCC policy. However, this does not create a security problem because these HBAs cannot contact any device outside of their immediate loop.

DCC policies must follow the naming convention "DCC_POLICY_*nnn*," where *nnn* represents a unique string. To save memory and improve performance, one DCC policy per switch or group of switches is recommended.

Device ports must be specified by port WWN. Switch ports can be identified by the switch WWN, domain ID, or switch name followed by the port or area number. To specify an allowed connection, enter the device port WWN, a semicolon, and the switch port identification. Following are the possible methods of specifying an allowed connection:

- deviceportWWN;switchWWN (port or area number)
- deviceportWWN;domainID (port or area number)
- deviceportWWN;switchname (port or area number)

Table 13 lists the possible DCC policy states.

Table 13: DCC Policy States

Policy State	Characteristics
No policy	Any device can connect to any switch port in the fabric.
Policy with no entries	Any device can connect to any switch port in the fabric. An empty policy is the same as no policy.
Policy with entries	If a device WWN is specified in a DCC policy, that device is only allowed access to the fabric if connected to a switch port listed in the same policy. If a switch port is specified in a DCC policy, it only permits connections from devices that are listed in the policy. Devices with WWNs that are not specified in a DCC policy are allowed to connect to the fabric at any switch ports that are not specified in a DCC policy. Switch ports and device WWNs may exist in multiple DCC policies.

Note: When a DCC violation occurs, the related port is automatically disabled and must be re-enabled using the `portenable` command.

Creating a DCC Policy

To create a DCC policy:

1. From a *sectelnet* or Secure Shell *session, log in to the* primary FCS switch as admin.
2. Enter the following:

   ```
   secpolicycreate "DCC_POLICY_nnn",
   "member;...;member"
   ```

   DCC_POLICY_nnn is the name of the DCC policy to be created; nnn is a string consisting of up to 19 alphanumeric or underscore characters to differentiate it from any other DCC policies.

   Member contains device and switch port information: deviceportWWN;switch(port):

   — "deviceportWWN" is the WWN of the device port.

   — "switch" can be the switch WWN, domain ID, or switch name. The port can be specified by port or area number. Designating ports automatically includes the devices currently attached to those ports. The ports can be specified using any of the following syntax methods:

- (1-6)Selects ports 1 through 6.
- (*)Selects all ports on the switch.
- [*]Selects all ports and all devices attached to those ports.
- [3, 9]Selects ports 3 and 9 and all devices attached to those ports.
- [1-3, 9]Selects ports 1, 2, 3, 9, and all devices attached to those ports.

3. To save or activate the new policy, enter either the `secpolicysave` or the `secpolicyactivate` command.

   If either of these commands is not entered, the changes are lost when the session is logged out. For more information about these commands, see "Saving Changes to Secure Fabric OS Policies" on page 97 and "Activating Changes to Secure Fabric OS Policies" on page 98.

   Examples

   Creating a DCC policy "DCC_POLICY_server" that includes device "11:22:33:44:55:66:77:aa" and port 1 and port 3 of switch domain 1:

```
primaryfcs:admin> secPolicyCreate "DCC_POLICY_server",
"11:22:33:44:55:66:77:aa;1(1,3)"
DCC_POLICY_xxx has been created
primaryfcs:admin>
```

   Creating a DCC policy "DCC_POLICY_storage" that includes device port WWN "22:33:44:55:66:77:11:bb," all ports of switch domain 2, and all currently connected devices of switch domain 2:

```
primaryfcs:admin> secPolicyCreate "DCC_POLICY_storage",
"22:33:44:55:66:77:11:bb;2[*]"
DCC_POLICY_xxx has been created
primaryfcs:admin>
```

   Creating a DCC policy "DCC_POLICY_abc" that includes device "33:44:55:66:77:11:22:cc" and ports 1-6 and port 9 of switch domain 3:

```
primaryfcs:admin> secPolicyCreate "DCC_POLICY_abc",
"33:44:55:66:77:11:22:cc;3(1-6,9)"
DCC_POLICY_xxx has been created
primaryfcs:admin>
```

Creating a DCC policy “DCC_POLICY_example” that includes devices 44:55:66:77:22:33:44:dd and 33:44:55:66:77:11:22:cc, ports 1-4 of switch domain 4, and all devices currently connected to ports 1-4 of switch domain 4:

```
primaryfcs:admin> secPolicyCreate "DCC_POLICY_example",
"44:55:66:77:22:33:44:dd;33:44:55:66:77:11:22:cc;4[1-4]"
DCC_POLICY_xxx has been created
primaryfcs:admin>
```

Creating an SCC Policy

The SCC policy is used to restrict which switches can join the fabric. Switches are checked against the policy each time Secure Mode is enabled, the fabric is initialized with Secure Mode enabled, or an E_Port-to-E_Port connection is made.

The policy is named SCC_POLICY, and accepts members listed as WWNs, domain IDs, or switch names. Only one SCC policy may be created.

By default, any switch is allowed to join the fabric; the SCC policy does not exist until it is created by the administrator.

Note: When an SCC policy is activated, any non-FCS switches in the fabric not included in the policy member list, will be segmented from the fabric.

Table 14 lists possible SCC policy states.

Table 14: SCC Policy States

Policy State	SCC Policy Enforcement
No policy specified	All switches may join the fabric.
Policy specified, but with no members	The SCC policy includes all FCS switches. All non-FCS switches are excluded. Only FCS switches may join the fabric.
Policy specified, with members	The SCC policy contains all FCS switches and any switches specified in the member list. Any non-FCS switches not explicitly specified are excluded. Only FCS switches and explicitly specified non-FCS switches may join the fabric.

To create an SCC policy:

1. Log in to the primary FCS switch as admin from a *sectelnet* or Secure Shell *session.*
2. Enter the following:

   `secpolicycreate "policy_name", "member;...;member"`

   Policy_name is MS_POLICY.

   Member is a device WWN.
3. To save or activate the new policy, enter either the `secpolicysave` or the `secpolicyactivate` command.

If either of these commands is not entered, the changes are lost when the session is logged out. For more information about these commands, see "Saving Changes to Secure Fabric OS Policies" on page 97 and "Activating Changes to Secure Fabric OS Policies" on page 98.

Example

Creating an SCC policy that allows switches that have domain IDs 2 and 4 to join the fabric:

```
primaryfcs:admin> secPolicyCreate "SCC_POLICY", "2;4"
SCC_POLICY has been created
primaryfcs:admin>
```

Managing Secure Fabric OS Policies

All Secure Fabric OS transactions can be performed through the primary FCS switch only, except for the `sectransabort`, `secfcsfailover`, `secstatsreset`, and `secstatsshow` commands.

Multiple sessions can be created to the primary FCS switch from one or more hosts. However, the software allows only one Secure Fabric OS transaction at a time. If a second Secure Fabric OS transaction is started, it fails. The only secondary transaction that can succeed is the `sectransabort` command.

All policy modifications are only saved in volatile memory until the changes are saved or activated.

The following functions can be performed on existing Secure Fabric OS policies:

- "Saving Changes to Secure Fabric OS Policies" on page 97

  Save changes to flash memory actually implementing the changes within the fabric. This saved but inactive information is known as the "defined policy set."

- "Activating Changes to Secure Fabric OS Policies" on page 98

  Simultaneously save and implement all the policy changes made since the last time changes were activated. The activated policies are known as the "active policy set."

- "Adding a Member to an Existing Policy" on page 98

  Add one or more members to a policy. The aspect of the fabric covered by each policy is closed to access by all devices/switches that are not listed in that policy.

- "Removing a Member from a Policy" on page 99

  Remove one or more members from a policy. If all members are removed from a policy, that aspect of the fabric becomes closed to all access. The last member of the FCS_POLICY cannot be removed, because a primary FCS switch must be designated.

- "Deleting a Policy" on page 100

  Delete an entire policy; however, keep in mind that doing so opens up that aspect of the fabric to all access.

- "Aborting All Uncommitted Changes" on page 101

  Abort all the changes to the Secure Fabric OS policies since the last time changes were saved or activated.

- "Aborting a Secure Fabric OS Transaction" on page 102

  From any switch in the fabric, abort a Secure Fabric OS-related transaction that has become frozen (such as due to a failed host) and that is preventing other Secure Fabric OS transactions.

Each of these tasks is described in the subsections that follow.

Saving Changes to Secure Fabric OS Policies

You can save changes to Secure Fabric OS policies without activating them by entering the `secpolicysave` command. This saves the changes to the defined policy set.

Note: Until the `secpolicysave` or `secpolicyactivate` command is issued, all policy changes are in volatile memory only and are lost if the switch reboots or the current session is logged out.

To save changes to the Secure Fabric OS policies without activating the changes:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the `secpolicysave` command.

   Example

```
primaryfcs:admin> secPolicySave
Committing configuration...done.
Saving Define FMPS ...
done
primaryfcs:admin>
```

Activating Changes to Secure Fabric OS Policies

Changes to the Secure Fabric OS policies can be implemented using the `secpolicyactivate` command. This saves the changes to the active policy set and activates all policy changes since the last time the command was issued. Policies cannot be activated on an individual basis; all changes to the entire policy set are activated by the command.

Note: Until a `secpolicysave` or `secpolicyactivate` command is issued, all policy changes are in volatile memory only and are lost upon rebooting.

To activate changes to the Secure Fabric OS policies:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the `secpolicyactivate` command.

Example

```
primaryfcs:admin> secPolicyActivate
About to overwrite the current Active data.
ARE YOU SURE (yes, y, no, n): [no] y
Committing configuration...done.
Saving Defined FMPS ...
done
Saving Active FMPS ...
done
primaryfcs:admin>
```

Adding a Member to an Existing Policy

You can add members to policies using the `secpolicyadd` command. As soon as a policy has been created, the aspect of the fabric managed by that policy is closed to access by all devices that are not listed in the policy.

To add a member to an existing Secure Fabric OS policy:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.

2. Enter the following:

   `secpolicyadd "policy_name", "member;...;member"`

   Policy_name is the name of the Secure Fabric OS policy.

   Member is the item to be added to the policy, identified by device or switch IP address, switch domain ID, device or switch WWN, or switch name.

3. To implement the change immediately, enter the `secpolicyactivate` command.

   Examples

   Adding a member to the MS_POLICY using the device port WWN:

```
primaryfcs:admin> secPolicyAdd "MS_POLICY", "12:24:45:10:0a:67:00:40"
Member(s) have been added to MS_POLICY.
primaryfcs:admin>
```

   Adding an SNMP manager to WSNMP_POLICY:

```
primaryfcs:admin> secPolicyAdd "WSNMP_POLICY", "192.168.5.21"
Member(s) have been added to WSNMP_POLICY.
primaryfcs:admin>
```

   Adding two devices to the DCC policy, to attach domain 3 ports 1 and 3 (WWNs of devices are 11:22:33:44:55:66:77:aa and 11:22:33:44:55:66:77:bb):

```
primaryfcs:admin> secPolicyAdd "DCC_POLICY_abc",
"11:22:33:44:55:66:77:aa;11:22:33:44:55:66:77:bb;3(1,3)"
primaryfcs:admin>
```

Removing a Member from a Policy

If all the members are removed from a policy, that policy becomes closed to all access. The last member cannot be removed from the FCS_POLICY, because a primary FCS switch must be designated.

To remove a member from a Secure Fabric OS policy:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.

2. Enter the following:

   `secpolicyremove "policy_name", "member;...;member"`

   Policy_name is the name of the Secure Fabric OS policy.

   Member is the device or switch to be removed from the policy, identified by IP address, switch domain ID, device or switch WWN, or switch name.

3. To implement the change immediately, enter the `secpolicyactivate` command.

   Example

   Removing a member that has a WWN of 12:24:45:10:0a:67:00:40 from MS policy:

```
primaryfcs:admin> secPolicyRemove "MS_POLICY",
"12:24:45:10:0a:67:00:40"
Member(s) have been removed from MS_POLICY. .
primaryfcs:admin>
```

Deleting a Policy

If an entire Secure Fabric OS policy is deleted, that aspect of the fabric becomes open to all access.

To delete a Secure Fabric OS policy:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the following:

   `secpolicydelete "policy_name"`

   policy_name is the name of the Secure Fabric OS policy.

3. To implement the change immediately, enter the `secpolicyactivate` command.

Note: The FCS_POLICY cannot be deleted.

Example

```
primaryfcs:admin> secPolicyDelete "MS_POLICY"
About to delete policy MS_POLICY.
Are you sure (yes, y, no, n):[no] y
MS_POLICY has been deleted.
primaryfcs:admin>
```

Aborting All Uncommitted Changes

The `secpolicyabort` command can be used to abort all Secure Fabric OS policy changes that have not yet been saved. This function can only be performed from the primary FCS switch.

To abort all unsaved changes:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the `secpolicyabort` command.

   All changes since the last time the `secpolicysave` or `secpolicyactivate` commands were entered are aborted.

   Example

```
primaryfcs:admin> secPolicyAbort
Unsaved data has been aborted.
primaryfcs:admin>
```

Aborting a Secure Fabric OS Transaction

You can use the `sectransabort` command to abort a single Secure Fabric OS transaction from any switch in the fabric. This makes it possible to abort a transaction that has become frozen due to a failed host. If the switch itself fails, the transaction aborts by default. This command cannot be used to abort an active transaction.

To abort a Secure Fabric OS transaction:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the `sectransabort` command. Any Secure Fabric OS transaction that was in process is aborted (except for the transaction of entering this command).

Example

```
primaryfcs:admin> secTransAbort
Transaction has been aborted.
primaryfcs:admin>
```

Managing Secure Fabric OS

4

This chapter contains the following sections:

Overview

Secure Fabric OS can be managed through Fabric Manager and *sectelnet*. In addition, Secure Shell is supported for Fabric OS v4.2.x. When Secure Mode is enabled for a fabric, all Secure Fabric OS administrative operations, all Zoning commands, and some Management Server commands must be executed on the primary FCS switch. For a list of the command and related restrictions, see "Command Restrictions in Secure Mode" on page 140.

Viewing Secure Fabric OS Information

The following Secure Fabric OS information is available:

- General Secure Fabric OS-related information about a fabric
- Secure Fabric OS policy sets (active and defined)
- Information about one or more Secure Fabric OS policies

For information about viewing the Secure Fabric OS statistics, see "Displaying and Resetting Secure Fabric OS Statistics" on page 110.

Displaying General Secure Fabric OS Information

The `secfabricshow` command can be used to display general Secure Fabric OS related information about a fabric.

To display general Secure Fabric OS-related information:

1. Open a *sectelnet* or Secure Shell session to the primary FCS switch and log in as admin.
2. Enter the `secfabricshow` command. The command displays the switches in the fabric and their status (Ready, Error, Busy, NoResp for no response from the switch).

   Example

```
primaryfcs:admin> secfabricshow
Role    WWN                     DId Status  Enet IP Addr    Name
==========================================================
non-FCS 10:00:00:60:69:10:03:23   1 Ready   192.168.100.148 "nonfcs"
Backup  10:00:00:60:69:00:12:53   2 Ready   192.168.100.147 "backup"
Primary 10:00:00:60:69:22:32:83   3 Ready   192.168.100.135 "primaryfcs"
__________________________________________________________________

Secured switches in the fabric: 3
primaryfcs:admin>
```

Viewing the Secure Fabric OS Policy Database

The `secpolicydump` command can be used to display the Secure Fabric OS policy database, which consists of the active and defined policy sets. This command displays information without page breaks.

To view the Secure Fabric OS policy database:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the following:

   `secpolicydump "listtype", "policy_name"`

   Listtype is the type of Secure Fabric OS policy set.

   Policy_name is the name of the Secure Fabric OS policy. If you do not specify a policy name, the command displays all the policies in the specified policy set.

   If you do not specify any operands, the command displays all policies in both the active and defined policy sets.

   Example

   Displaying all policies in both active and defined policy sets:

```
primaryfcs:admin> secPolicyDump

_____________________________________________________
                 DEFINED POLICY SET
FCS_POLICY
Pos Primary WWN DId swName
_____________________________________________________
1 Yes 10:00:00:60:69:30:15:5c 1 primaryfcs
HTTP_POLICY
IpAddr
_____________________________________________________
192.155.52.0
_____________________________________________________
_____________________________________________________
                  ACTIVE POLICY SET
FCS_POLICY
Pos Primary WWN DId swName
_____________________________________________________
1 Yes 10:00:00:60:69:30:15:5c 1 primaryfcs
HTTP_POLICY
IpAddr
_____________________________________________________
192.155.52.0
192.155.53.1
192.155.54.2
192.155.55.3
_____________________________________________________
primaryfcs:admin>
```

Displaying Individual Secure Fabric OS Policies

The `secpolicyshow` command can be used to view information about one or more specified Secure Fabric OS policies. This command displays information, with page breaks.

To display information about a specific Secure Fabric OS policy:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the following:

   `secpolicyshow` *"listtype", "policy_name"*

   Listtype is the type of Secure Fabric OS policy set. It can be *active, defined,* or an asterisk (*), which displays both versions of the specified policy.

   Policy_name is the name of the Secure Fabric OS policy. If you do not specify a policy name, the command displays all the policies in the specified policy set.

   If you do not specify any operands, the command displays all policies in both the active and defined policy sets.

   Example

   Showing all policies in the defined policy set:

```
primaryfcs:admin> secpolicyshow "defined"
_____________________________________________________
              DEFINED POLICY SET

FCS_POLICY
   Pos   Primary WWN                     DId swName
   _____________________________________________________
     1   Yes     10:00:00:60:69:30:15:5c   1 primaryfcs

HTTP_POLICY
   IpAddr
   _____________________________________________________
   192.155.52.0
   192.155.53.1
   192.155.54.2
   192.155.55.3
   192.155.56.4


_____________________________________________________
primaryfcs:admin>
```

Showing the active version of the FCS policy:

```
primaryfcs:admin> secPolicyshow "active","FCS_POLICY"
_____________________________________________________
               ACTIVE POLICY SET

FCS_POLICY
   Pos   Primary WWN                    DId swName
   _____________________________________________
     1   Yes     10:00:00:60:69:30:15:5c   1 primaryfcs


_____________________________________________________
primaryfcs:admin>
```

Displaying Status of Secure Mode

The `secmodeshow` command can be used to determine whether Secure Mode is enabled.

To determine whether Secure Mode is enabled:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch and log in as admin.
2. Enter the `secmodeshow` command. The command displays the status of Secure Mode, the version number and time stamp, and the list of switches in the FCS policy.

   Example

```
primaryfcs:admin> secmodeshow
Secure Mode: ENABLED.
Version Stamp: 10354, Thu Oct  4 10:23:32 2001.
Pos   Primary WWN                    DId swName.
================================================
1   Yes     10:00:00:60:69:11:fc:53   2 primaryfcs.
2   No      10:00:00:60:69:11:fc:55   1 backupswitch.
primaryfcs:admin>
```

Table 15 lists the information that displays if Secure Mode is enabled.

Table 15: Secure Mode Information

Item	Indicates
Pos	Position of switch in FCS list
Primary	"Yes" if switch is primary FCS, "no" if not
WWN	WWN of each FCS switch
DId	Domain ID of each FCS switch
swName	Switch name of each FCS switch

Displaying and Resetting Secure Fabric OS Statistics

Secure Fabric OS provides several statistics regarding attempted policy violations. This includes events such as the following:

- A DCC policy exists that defines which devices are authorized to access which switch (port) combinations, and a device that is not listed in the policy tries to access one of the defined switch (port) combinations.
- An attempt is made to log in to an account with an incorrect password.

The statistics for all DCC policies are added together.

Note: Rebooting the switch resets all the statistics. Secure Fabric OS statistics can also be monitored through Fabric Watch.

Each statistic indicates the number of times the monitored event has occurred since the statistics were last reset (`secstatsreset` command). For the Telnet policy, this includes all the automated login attempts made by the *sectelnet* or Secure Shell client software, in addition to the actual attempts made by the user.

Table 16 lists Secure Fabric OS statistics and their definitions.

Table 16: Secure Fabric OS Statistics

Statistic	Definition
TELNET_POLICY	The number of attempted violations to the Telnet policy (includes automated attempts made by client software).
HTTP_POLICY	The number of attempted violations to the HTTP policy.
API_POLICY	The number of attempted violations to the API policy (includes automated attempts made by client software).
RSNMP_POLICY	The number of attempted violations to the RSNMP policy.
WSNMP_POLICY	The number of attempted violations to the WSNMP policy.
SES_POLICY	The number of attempted violations to the SES policy.
MS_POLICY	The number of attempted violations to the MS policy.
SERIAL_POLICY	The number of attempted violations to the Serial policy.
FRONTPANEL_POLICY	The number of attempted violations to the Front Panel policy.
SCC_POLICY	The number of attempted violations to the SCC policy.

Table 16: Secure Fabric OS Statistics (Continued)

Statistic	Definition
DCC_POLICY	The number of attempted violations to the DCC policy. **Note:** Fabric OS v4.2.x increases the counter by 1 for each drive in a JBOD; Fabric OS v3.1.2 increases the counter by 1 for the entire JBOD.
LOGIN	The number of invalid login attempts.
INVALID_TS (invalid timestamps)	A received packet has a time stamp that differs from the time of the receiving switch by more than the maximum allowed difference.
INVALID_SIGN (invalid signatures)	A received packet has a bad signature.
INVALID_CERT (invalid certificates)	A received certificate is not properly signed by the root CA of the receiving switch.
SLAP FAIL (SLAP* failures)	The switch received a SLAP that it could not verify, possibly due to bad certificates, bad signature, the other side not performing SLAP, or SLAP packets that were received out of sequence. This counter is not advanced if SLAP protocol does not complete, which can happen when a switch that does not have Secure Mode enabled is attached to a switch that does.
SLAP_BAD_PKT (SLAP* bad packets)	SLAP packets are received with a bad transaction ID.
TS_OUT_SYNC (TS out of synchronization)	The time server is out of synchronization with the primary FCS switch.
NO_FCS (no fabric configuration server)	The number of times the switch has simultaneously lost contact with all the switches in the FCS list.
INCOMP_DB (incompatible Secure Fabric OS database)	Secure Fabric OS databases are incompatible; might be due to different version numbers, time stamps, FCS policies, or Secure Mode status.
ILLEGAL_CMD (illegal command)	The number of times a command is issued on a switch where it is not allowed (such as entering `secmodedisable` on a non-FCS switch).

Displaying Secure Fabric OS Statistics

The `secstatsshow` command can be used to display statistics for one or all Secure Fabric OS policies, depending on the operand entered. This command can only be issued from the primary FCS switch if the "list" operand is specified. If the "list" operand is not specified, this command can be entered from any switch in the fabric.

To display Secure Fabric OS statistics:

1. Log in to the primary FCS switch as admin from a *sectelnet* or Secure Shell session.
2. Enter the following:

   `secstatsshow "name", "list"`

   Name is the name of a Secure Fabric OS statistic or the policy that relates to the statistic. The valid statistic names are listed in Table 16. An asterisk (*) can be entered to indicate all statistics.

   List is a list of the Domain IDs for which to display the statistics. You can enter an asterisk (*) to indicate all switches in the fabric. The default value is that of the local switch.

   If neither operand is specified, all statistics for all policies are displayed.

   The statistic and number of related attempted policy violations are displayed.

   Example

   Displaying Secure Fabric OS statistics for the Management Server policy:

```
primaryfcs:admin> secstatsshow "MS_POLICY"
Name Value
====================
MS 20
primaryfcs:admin>
```

Resetting Secure Fabric OS Statistics

The `secstatsreset` command can be used to reset statistics for a particular policy or all policies to 0. This command can be issued on any switch. Recording and resetting the statistics allows you to identify changes in traffic patterns since the statistics were last reset. This command can only be issued from the primary FCS switch if the "list" operand is specified. If the "list" operand is not specified, this command can be entered from any switch in the fabric.

To reset a statistic counter to 0:

1. Log in to the primary FCS switch as admin from a *sectelnet* or Secure Shell session.
2. If desired, enter the `secstatsshow` command and record the current statistics.
3. Reset the statistics by entering the following:

   `secstatsreset "name", "list"`

   Name is the name of the statistic or the policy that relates to the statistic. The valid statistic names are listed in Table 16. You can enter an asterisk (*) to indicate all Secure Fabric OS statistics.

   List is a list of the Domain IDs for which to reset the statistics. You can enter an asterisk (*) to indicate all switches in the fabric. The default value is that of the local switch.

   If neither operand is specified, all statistics for all Secure Fabric OS policies are reset to 0.

   The specified statistics are reset to 0.

   Example

   Resetting all statistics on a local switch:

```
primaryfcs:admin> secstatsreset
About to reset all security counters.
Are you sure (yes, y, no, n):[no] y
Security statistics reset to zero.
primaryfcs:admin>
```

   Resetting the DCC_POLICY statistics on domains 1 and 69:

```
primaryfcs:admin> secstatsreset "DCC_POLICY", "1;69"
Reset DCC_POLICY statistic.
primaryfcs:admin>
```

Managing Passwords

When Secure Mode is enabled, the following conditions apply:

- The `passwd` command can only be entered on the primary FCS switch.
- The root and factory accounts can only be accessed from the FCS switches. Attempting to access them from a non-FCS switch generates an error message.
- The admin account remains available from all switches, but two passwords are implemented: one for all FCS switches and one for all non-FCS switches.
- Temporary passwords can be created for specific switches, making it possible to provide temporary access to another user.

The user account remains available fabric-wide regardless of whether Secure Mode is enabled. The characteristics of the different accounts when Secure Mode is enabled and disabled are described in Table 17.

If a digital certificate is installed, the *sectelnet*, API, and HTTP passwords are automatically encrypted, regardless of whether Secure Mode is enabled.

Note: Record passwords and store them in a secure place; recovering passwords can require significant effort and result in fabric downtime.

Table 17: Login Account Behavior with Secure Mode Disabled and Enabled

Login Account	Secure Mode Disabled	Secure Mode Enabled
Admin Recommended for all administrative options. Can use to modify admin and user passwords.	Available on all switches. Password is specific to each switch; can modify using `passwd` command.	Available on all switches. Can create temporary passwords. Two passwords: • One for all FCS switches; can modify using `passwd` command on the primary FCS switch. • One for all non-FCS switches; can modify using `secnonfcspasswd` command on the primary FCS switch.
Factory Created for switch initialization purposes; not recommended for administrative operations. Can use to modify factory, admin, and user passwords.	Available on all switches. Password is specific to each switch; can modify using `passwd` command.	Available on FCS switches only. However, can temporarily enable root and factory accounts on non-FCS switches by creating a temporary password. Password is common to all FCS switches; can modify using `passwd` command on the primary FCS switch.
Root Creating for debugging purposes; not recommended for administrative operations. Can use to modify root, factory, admin, and user passwords.	Available on all switches. Password is specific to each switch; can modify using `passwd` command.	Available on FCS switches only. However, can temporarily enable root and factory accounts on non-FCS switches by creating a temporary password. Password is common to all FCS switches; can modify using `passwd` command on the primary FCS switch.

Modifying Passwords in Secure Mode

The `passwd` command can be used to modify the fabric-wide user password and the passwords for the FCS switches. The `secnonfcspasswd` can be used to modify the admin password for non-FCS switches.

Note: If the password is changed for a login account, all open sessions using that account are terminated, including the session from which the `passwd` command was executed, if applicable

Modifying the FCS Switch Passwords or the Fabric-Wide User Password

The `passwd` command can be used to modify the passwords for the following accounts when Secure Mode is enabled:

- The fabric-wide user account
- The admin, root, and factory accounts on the FCS switches

To modify the passwords:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin, root, or factory, depending on which password you want to modify (use the account for which you want to modify a password or a higher-level account).
2. Enter the `passwd` command.
3. Enter the new passwords at the prompts. The passwords can be anywhere from 8 to 40 alphanumeric characters.

   The passwords are distributed to all switches in the fabric and saved in the Secure Fabric OS database. Any existing telnet connections to the switches are terminated and must be reinitiated if access is required.

   Example

```
primaryfcs:admin> passwd
For username - admin
Old password:
New password:
Re-enter new password:
For username - user
New password:
Re-enter new passwd:
primaryfcs:admin>
```

Modifying the Non-FCS Switch Admin Password

The `secnonfcspasswd` command can be used to modify the password for the admin account on non-FCS switches. Secure Mode must be enabled to use this command.

To modify the admin password for non-FCS switches:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the `secnonfcspasswd` command.
3. Enter the new non-FCS admin password at the prompt. The password can be anywhere from 8 to 40 alphanumeric characters.

   This password becomes the admin password for all non-FCS switches in the fabric.
4. Reenter the new non-FCS admin password at the prompt. The password is distributed to all switches in the fabric and saved in the Secure Fabric OS database. Any existing admin-level telnet connections to these non-FCS switches are terminated.

   Example

```
primaryfcs:admin> secnonfcspasswd
Non FCS switch password:
Re-enter new password:
Committing configuration...done.
primaryfcs:admin>
```

Using Temporary Passwords

Temporary passwords can be created to grant temporary access to a specific switch and login account without compromising the confidentiality of the regular passwords; the regular passwords also remain in effect. Temporary passwords can be removed; they are also automatically lost after a switch reboot.

Note: If a temporary password is set on a backup FCS switch, and the backup FCS switch then becomes the primary FCS switch, the temporary password remains in effect on that switch until the `sectemppasswdreset` command is entered.

Creating a Temporary Password for a Switch

The `sectemppasswdset` command can be used to create a temporary password. You must specify a login account and a switch Domain ID.

To create a temporary admin password on a non-FCS switch:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the following:

   `sectemppasswdset` *`domain, "login_name"`*

   Domain is the Domain ID of the switch for which you want to set a temporary password.

   Login_name is the login account for which you want to set the temporary password.
3. Enter the admin password at the prompt.
4. Enter an alphanumeric password between 8 and 40 characters in length.
5. Reenter the password exactly as entered the first time.

   Example

   Creating a temporary password for the admin account on a switch that has a Domain ID of 2:

```
primaryfcs:admin> sectemppasswdset 2, "admin"
Set remote switch admin password: swimming
Re-enter remote switch admin password: swimming
Committing configuration........done
Password successfully set for domain 2 for admin.
primaryfcs:admin>
```

Removing a Temporary Password from a Switch

The `sectemppasswdreset` command can be used to remove the temporary password. The regular password remains in effect.

To remove the temporary password from a switch:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the following:

   `sectemppasswdreset` *`domain, "login_name"`*

Domain is the Domain ID of the switch for which you want to remove the temporary password.

Login_name is the login account to which the temporary password applies.

You can enter the command with no parameters to reset all temporary passwords in the fabric.

Removing a temporary password for the admin account from a switch that has a Domain ID of 2:

```
switch:admin> sectemppasswdreset 2, "admin"
Committing configuration.....done
Password successfully reset on domain 2 for admin
switch:admin>
```

Resetting the Version Number and Time Stamp

When a change is made to any information in the Secure Fabric OS database (zoning, policies, passwords, or SNMP), the current time stamp and a version number are attached to the Secure Fabric OS database.

This information is used to determine which database is preserved when two or more fabrics are merged. The database of the fabric with a non-zero version stamp is kept. When merging fabrics, ensure that the time stamp of the database you want to preserve is nonzero; then, set the time stamp of all other fabrics to 0. To ensure that the time stamp of a fabric is nonzero, modify a policy and enter the `secpolicysave` or `secpolicyactivate` command.

To display the version number and time stamp of a fabric:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the `secmodeshow` command.

To reset the time stamp of a fabric to 0:

1. From a *sectelnet* or Secure Shell session, log in to the primary FCS switch as admin.
2. Enter the `secversionreset` command. If the fabric contains no FCS switch, you can enter the `secversionreset` command on any switch.

Adding Switches and Merging Fabrics with Secure Mode Enabled

To merge fabrics, all switches must be in the same state regarding Secure Mode and must have an identical FCS policy. Any switches that do not have a matching FCS policy or are in a different state regarding Secure Mode are segmented. For example, two fabrics that both have Secure Mode disabled can be merged, and two fabrics that both have Secure Mode enabled can be merged.

When fabrics are merged, the fabric that contains the desired configuration information must have a non-zero stamp, and all the other fabrics being merged must have 0 version stamps. The Security policy set, zoning configuration, password information, and SNMP community strings are overwritten by the fabric whose version stamp is nonzero. Before merging, verify that the fabric that contains all the desired information has the nonzero stamp.

Note: For general information about merging fabrics and instructions for merging fabrics that are not in Secure Mode, refer to the *HP StorageWorks Fabric OS 4.2.x Procedures User Guide*.

Table 18 lists the results of moving switches in and out of fabrics with Secure Mode enabled or disabled.

Table 18: Results from Enabling or Disabling Secure Mode in the SAN

Initial State of Switch	If set up as a standalone switch	If moved into a fabric that has Secure Mode enabled and a functioning primary FCS switch	If moved into a fabric that has Secure Mode enabled but no FCS switches are available:	If moved into a non-secure fabric:
Has Secure Mode enabled and is primary FCS switch in the FCS policy stored on switch.	Forms a one switch fabric with Secure Mode enabled, and acts as primary FCS switch.	Segments unless FCS policies are identical. If identical, switch is primary FCS switch unless other FCS switch is higher in the FCS policy.	Segments unless FCS policies are identical. If policies are identical, switch becomes primary FCS switch.	Segments from fabric.
Has Secure Mode enabled and is backup FCS switch in the FCS policy stored on switch.	Forms a one switch fabric with Secure Mode enabled, and acts as primary FCS switch.	Segments unless FCS policies are identical. If policies are identical, switch is backup FCS switch.	Segments unless FCS policies are identical. If policies are identical, switch becomes primary FCS switch.	Segments from fabric.
Has Secure Mode enabled and is non-FCS switch in the FCS policy stored on switch.	Forms a one switch fabric with Secure Mode enabled but no FCS switch (to specify primary FCS switch, enter `secmodeenable`).	Segments unless FCS policies are identical. If policies are identical, switch is non-FCS switch.	Segments; cannot join fabric until a primary FCS switch is available (to specify primary FCS switch, enter `secmodeenable`).	Segments from fabric.
Has Secure Mode disabled.	Standard operation.	Segments from fabric.	Segments from fabric.	Standard operation.

Note: Although the following procedure does not require rebooting the fabric, there is potential for segmentation or other disruption to the fabric due to the number of factors involved in the merge process.

To merge two or more fabrics that have Secure Fabric OS implemented:

1. As a precaution, back up the configuration of each fabric to be merged by entering the `configupload` command and completing the prompts. This also backs up the policies if Secure Fabric OS was already in use on the switch.
2. Ensure that all switches to be merged are running Fabric OS v2.6.2, v3.1.2, or v4.2.x:
   a. Open a CLI connection (serial or telnet) to one of the switches in the fabric.
   b. Log in to the switch as admin. The default password is "password".
   c. Enter the `version` command. If the switch is a Core Switch 2/64 or SAN Director 2/128, you can alternatively enter the `firmwareshow` command.
   d. If the switch is not running Fabric OS v2.6.2, v3.1.2, or v4.2.x, upgrade the firmware as required. For information on upgrading firmware, refer to the *HP StorageWorks Fabric OS 4.2.x Procedures User Guide*.
   e. Customize the account passwords from the default values, as described in "Customizing the Account Passwords" on page 35.
   f. Repeat for each switch that you intend to include in the final merged fabric.
3. If the final merged fabric will contain switches running Fabric OS v2.6.2 or v3.1.2 and switches running Fabric OS v4.2.x, the PID mode on all switches must be compatible; for more information about PID modes, refer to the *HP StorageWorks Fabric OS 4.2.x Procedures User Guide.*

Note: Changing the PID format causes an update to the DCC policies. If you change the PID format, use the `configdownload` command to create a new backup configuration file. Do not upload the old file.

4. Ensure that the Management Server Platform Service is consistently enabled or disabled across all the switches to be merged. For information about Management Server support provided by Fabric OS, refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide*.
5. Ensure that all switches to be merged have activated Secure Fabric OS and Zoning licenses, as described in "Verifying or Activating the Secure Fabric OS and Zoning Licenses" on page 35.
6. Ensure that all switches to be merged have the required PKI objects (private key passphrase, switch private key, CSR, root certificate) and a digital certificate installed:
   a. Log in to the switch as admin.
   b. Enter the command supported by the Fabric OS installed on the switch:
      — For Fabric OS v4.2.x, enter `pkishow`.
      — For Fabric OS v2.6.2 and v3.1.2, enter `configshow` **"`pki`"**.

   A list displays the PKI objects currently installed on the switch.

Note: "Root Certificate" is an internal PKI object. "Certificate" is the digital certificate.

   c. Verify that all the objects show **Exist**.

   If the digital certificate shows **Empty**, repeat the procedure provided in "Distributing Digital Certificates to the Switches" on page 43. If any of the PKI objects other than the digital certificate show **Empty**, you can either reboot the switch to automatically re-create the objects or re-create them as described in "Re-creating PKI Objects if Required" on page 49.

   d. Repeat for the remaining switches in the fabric.
7. Install a supported CLI client on the computer workstations that you will be using to manage the merged fabric. Supported CLI clients include *sectelnet* and Secure Shell and are discussed in Installing a Supported CLI Client on a Computer Workstation, page 60.
8. Enable Secure Mode on all switches to be merged by entering the `secmodeenable` command on the primary FCS switches of any fabrics that do not already have Secure Mode enabled. For more information about enabling Secure Mode, refer to "Enabling Secure Mode" on page 66.

9. Determine which switches you want to designate as the primary FCS switch and backup FCS switches for the merged fabric; then, modify the FCS policy for *each* fabric to list these switches as the primary FCS switch and backup FCS switches. Ensure that all the FCS policies are an *exact* match; they must list the same switches, with the switches identified in the same manner and listed in the same order.

   If a fabric has become segmented with Secure Mode enabled but no FCS switches available, enter the `secmodeenable` command and modify the FCS policy to specify FCS switches. This is the only instance in which this command can be entered when Secure Mode is already enabled.

10. Modify the SCC policy on the final primary FCS switch (the one that will succeed as the primary FCS switch in the final merged fabric) to include all switches that are being merged.

11. Ensure that the final primary FCS switch has the desired Secure Fabric OS policy set, zoning configuration, password information, and SNMP community strings. The primary FCS switch will distribute this information fabric-wide.

12. Verify that the fabric that contains the final primary FCS switch has a non-zero version stamp by logging into the fabric and entering the `secModeShow` command. If this fabric does not show a non-zero version stamp, modify a policy and enter either the `secpolicysave` or `secpolicyactivate` command to create a non-zero stamp. Set the version stamp of the other fabrics to 0 by logging in to each fabric and entering the `secversionreset` command.

13. If fabrics are being rejoined after a segmentation, enter the `switchdisable` and `switchenable` commands on each switch that was segmented from the primary FCS switch. For each ISL connected to the segmented switch, enter the `portdisable` and `portenable` commands on both ISL ports.

14. Physically connect the fabrics. The fabrics automatically merge and the Secure Fabric OS configuration associated with the primary FCS switch that has the *non*zero stamp is kept.

Troubleshooting

Some of the most likely issues with Secure Fabric OS management and the recommended actions are described in Table 19. The information in the table is based on the assumption that the fabric was originally fully functional and Secure Mode was enabled.

Note: Some of the recommended actions might interrupt data traffic.

Table 19: Recovery Processes

Symptom	Possible Causes	Recommended Actions
Secure Fabric OS policies do not seem to be in effect.	Secure Mode is not enabled.	Enter the `secmodeshow` command. If Secure Mode is disabled, enter the `secmodeenable` command on the switch that you want to become the primary FCS switch and specify the FCS switches at the prompts.
	Policy changes have not been applied.	Enter the `secpolicyshow` command and review the differences between the active and defined policy sets. If desired, enter the `secpolicyactivate` command to activate all recent policy changes.
	Fabric has segmented.	See possible causes and actions for "One or more switches are segmented from the fabric," later in this table.

Table 19: Recovery Processes (Continued)

Symptom	Possible Causes	Recommended Actions
Commands cannot be executed from any switch in the fabric.	All FCS switches have failed but Secure Mode is still enabled, preventing access to fabric.	Enter the `secmodeenable` command from the switch that you want to become the new primary FCS switch, and specify the FCS switches. **Note**: Specify adequate backup FCS switches to prevent a recurrence of this problem.
Cannot access some or all switches in the fabric.	The MAC policies are restricting access. **Note:** An empty MAC policy blocks all access through that management channel.	Use a serial cable to connect to the primary FCS switch; then, enter the `secpolicyshow` command to review the MAC policies. Modify policies as necessary by either entering valid entries or deleting the empty policies.

Table 19: Recovery Processes (Continued)

Symptom	Possible Causes	Recommended Actions
Cannot access primary FCS switch by any management method.	Primary FCS switch has failed or has lost all connections.	Log in to the backup FCS switch that you want to become the new primary FCS switch and enter the `secfcsfailover` command to reassign the primary FCS role to a backup FCS switch. If no backup FCS switches are available, enter the `secmodeenable` command to specify a new primary FCS switch. Specify adequate backup FCS switches to prevent a recurrence. Troubleshoot the previous primary FCS switch as required.
A device or switch port listed in the SCC or in a DCC policy cannot be accessed.	Switch port might be disabled.	Enter the `switchshow` command. If the port in question is disabled, enter the `portenable` command. If the port still cannot be accessed, enter the `portenable` command for the port on the other switch.

Table 19: Recovery Processes (Continued)

Symptom	Possible Causes	Recommended Actions
One or more CLI sessions are automatically logged out.	Password might have been modified for login account in use, the `secmodeenable` command might have been issued, or switches might have changed switch roles (primary to backup, backup to primary and so forth).	Try closing and reopening CLI session.
On a Core Switch 2/64 or SAN Director 2/128, the CLI messages do not reflect switch status.	The CLI messages are pertaining to the other logical switch.	Verify switch or policy status by entering the `switchshow` or `secpolicyshow` commands.
CLI session freezes or cannot be established after Secure Mode is enabled.	CP card failed over and network routing cache require updating.	Try closing and reopening CLI session. If this fails, request that your LAN administrator refresh the network router cache.
A policy that has been created is not listed by the `secpolicyshow` command.	The new policy was not saved or activated.	Save or activate the policy changes by entering the `secpolicysave` or `secpolicyactivate` command.
	Incorrect policy name used.	Verify that the correct policy name was used. Policy names must be entered in all uppercase characters.

Table 19: Recovery Processes (Continued)

Symptom	Possible Causes	Recommended Actions
The message "The page cannot be displayed" is displayed when HTTP access is attempted, and response time is slow.	An HTTP policy has been created but has no members.	Add the desired members to the HTTP policy.
Unable to establish a *sectelnet*/SSH session to the IP address of the active CP card of a Core Switch 2/64 or SAN Director 2/128, or a session to the standby CP card is disconnected when it becomes the active CP card.	*Sectelnet*/SSH sessions cannot be established to the IP address of the active CP card in Secure Mode. This enables enforcement of Telnet policy for each logical switch.	Establish a *sectelnet*/SSH session to the IP addresses of the logical switches or the standby CP card instead (if allowed by Telnet policy).
A security transaction seems to have been lost.	One of the switches in the fabric rebooted while the transaction was in progress.	Wait for the switch to complete booting; then, reenter the security command on the new primary FCS switch to complete the transaction.
Fabric segments after Secure Mode is enabled.	CP cards failed over during process of enabling Secure Mode.	Enter `secmodeenable` again on the segmented switch, using the same FCS list as used before.

Table 19: Recovery Processes (Continued)

Symptom	Possible Causes	Recommended Actions
One or more switches are segmented from the fabric. **Note:** For instructions on rejoining fabrics, refer to the instructions in "Adding Switches and Merging Fabrics with Secure Mode Enabled" on page 121.	SCC_POLICY is excluding the segmented switches.	Use the `secpolicyadd` command on the primary FCS switch to add the switches to the SCC_POLICY.
	Management Server services on the segmented switches are inconsistent with rest of fabric.	Ensure that the Management Server Platform Service is consistently enabled or disabled across all the switches in the fabric.
	The segmented switches are missing PKI objects.	Determine the status of the PKI objects by following the procedure in "Verifying Installation of the Digital Certificates" on page 48. If any objects are missing, replace as described in "Re-creating PKI Objects if Required" on page 49.
	ISLs to the segmented switches are interrupted or a port failure occurred.	Check the hardware connections and the port status for all ISLs between the segmented switches and the fabric.
	Segmented switches diverged from rest of the fabric.	Disable the segmented switches, reset the configuration parameters to match the rest of the fabric, and reenable the switches.

Table 19: Recovery Processes (Continued)

Symptom	Possible Causes	Recommended Actions
When the SCC policy is created after a fabric segmentation, it automatically includes the segmented FCS switches.	The segmented FCS switches are still listed in the FCS policy.	Modify FCS policy to remove segmented FCS switches; then, modify or create the SCC policy as required.
Passwords that should be consistent across the fabric are not consistent.	A password recovery operation might have been performed on one or more switches.	To make the passwords the same, log in to the switch that had the password recovered and enter the `secversionreset` command, followed by `switchdisable` and `switchenable` commands.
Unsaved changes to the policies are lost.	The primary FCS switch might have failed over.	Reenter the changes; then, enter the `secpolicysave` or `secpolicyactivate` command.

Frequently Asked Questions

This section organizes the frequently asked questions into the following groups:

General

Is Secure Fabric OS standards-based?

— Yes. Secure Fabric OS uses standards-based security mechanisms and protocols.

Can you enable Secure Fabric OS on some switches but not others in the same fabric?

— No. Secure Fabric OS is enabled on a fabric-wide basis. All switches in the fabric must support Secure Fabric OS for it to be effective. Any switches that do not have Secure Fabric OS installed are segmented from the rest of the fabric.

How is Secure Fabric OS managed?

— Secure Fabric OS can be managed through the following methods:

  — A supported CLI client

  — Secure Fabric OS v2.6.2, v3.1.2, and v4.2.x support the *sectelnet* client. Secure Fabric OS v4.2.x also supports Secure Shell v2 clients.

  — Fabric Manager

  — Web Tools

  — Fabric Access (API)

Does Secure Fabric OS prevent all unauthorized access?

— There is no 100% protection in any network. However, the Secure Fabric OS product makes it possible for the administrator to create a significantly increased level of security that is customized to the fabric.

After Secure Fabric is turned on, can it be turned off again?

— Yes, by using the `secmodedisable` command. Turning Secure Mode off does not disrupt traffic.

What happens if I create a policy with no members in it?

— You cannot create an empty FCS Policy, but you can create other types of policies with no members. However, creating a policy with no members closes all access to that aspect of the fabric, which can result in preventing administrative access to the fabric. Before setting a policy, read all the information provided about that policy in "Creating Secure Fabric OS Policies Other than the FCS Policy" on page 76.

How do I prevent someone from adding a computer to the fabric and mounting a LUN?

— The following approaches can be used in conjunction, although no guarantees can be made of absolute security:

  — Store all the FCS switches in a physically secure area.

  — Use hardware-based zoning.

  — Create a DCC policy for each switch in the fabric.

  — Create an Options policy.

Management Access

What version of SSH and the SSH clients does Fabric OS v4.2.x support?

— Fabric OS v4.2.x supports version 2 of the SSH protocol. Use a SSH client that supports version 2 of the protocol such as OpenSSH or F-Secure.

Can I use standard telnet when Secure Mode is enabled?

— No, standard telnet is not supported when Secure Mode is enabled. However, *sectelnet* is available for Fabric OS v2.6.2, v3.1.2, and v4.2.x; SSH is also available for v4.2.x.

Is SSH part of the Secure Fabric OS feature?

— No, SSH is automatically included with Fabric OS v4.2.x, regardless of whether the Secure Fabric OS license is activated.

Digital Certificates and PKI Objects

What is PKI?

— PKI stands for Pubic Key Infrastructure; it refers to the use of cryptography to provide security (authentication, encryption, and so on.).

Can digital certificates be duplicated or installed on other switches?

— No; digital certificates correspond to the switch WWN and the private/public key pair generated by the switch.

Does the digital certificate have to be reinstalled if the motherboard is replaced?

— This depends on the version of Fabric OS on the new motherboard. Hardware shipped with Fabric OS v2.6.x, v2.6.1, v3.1.x, or v4.2.x automatically includes digital certificates. To determine whether the new motherboard already has a digital certificate, follow the instructions for verifying the PKI objects.

Do all switches already have a digital certificate?

— No, only switches that were shipped with v2.6.x, v2.6.1, v3.1.x, or v4.2.x installed have digital certificates.

How can I tell whether the digital certificate or PKI objects are available on a switch?

— For Fabric OS v4.2.x, enter the `pkishow` command. For earlier versions, enter `configshow "pki"`.

What happens if the PKI objects are deleted?

— PKI objects cannot be deleted in Secure Mode. If they are deleted when Secure Mode is disabled, Secure Mode cannot be reenabled until they are regenerated. If any PKI objects are missing, all the PKI objects should be deleted using the `pkiremove` command and then regenerated using the `pkicreate` command or by rebooting the switch (any missing PKI objects, except the digital certificate, are automatically regenerated when the switch is rebooted). If the digital certificate is deleted, it must be reinstalled on the switch according to the instructions provided in “Distributing Digital Certificates to the Switches” on page 43.

Are PKI objects required for any switch operations other than Secure Fabric OS?

— The PKI objects are only required for Secure Fabric OS and the *sectelnet* client.

Merging Fabrics

Which switch becomes the primary FCS switch when fabrics are merged?

— The first switch that is listed in the shared FCS policy for the merged fabric. If the FCS policies of the fabrics do not match before the merge, the fabrics segment.

What happens to the zoning information when fabrics are merged?

— The switch that becomes the primary FCS switch distributes the zoning information to all the switches in the newly merged fabric. Before merging fabrics, back up the zoning configurations and ensure that the switch that will become the primary FCS switch has the desired zoning configuration.

Passwords

What if I forget the root password?

— Refer to "Managing Passwords" on page 114 for general guidelines on password management. Refer to the password recovery information in the *HP StorageWorks Fabric OS 4.2.x Procedures User Guide*.

Secure Fabric OS Commands and Secure Mode Restrictions

This appendix provides the following information:

Secure Fabric OS Commands

The Secure Fabric OS commands provide the following capabilities:

- Enable and disable Secure Mode
- Fail over the primary FCS switch
- Create and modify Secure Fabric OS policies
- View all Secure Fabric OS-related information
- Modify passwords
- Create and remove temporary passwords
- View and reset Secure Fabric OS statistics
- View and reset version stamp information

Most Secure Fabric OS commands must be executed on the primary FCS switch when Secure Mode is enabled. For a list of restricted commands, see "Command Restrictions in Secure Mode" on page 140.

Table 20 lists all the commands available for managing Secure Fabric OS.

Table 20: Secure Fabric OS Commands

Command	Access Level	Description
`pkicreate`	Admin	Re-creates the PKI objects on the switch.
`pkiremove`	Admin	Removes the PKI objects from the switch.
`pkishow`	All users	Displays the status of the PKI objects and digital certificate on the switch.
`secactivesize`	Admin	Displays the size of the active Secure FOS database.
`secdefinesize`	Admin	Displays the size of the defined Secure FOS database.
`secfabricshow`	Admin	Displays Secure Fabric OS-related fabric information.
`secfcsfailover`	Admin	Transfers the role of the primary FCS switch to the next switch in the FCS policy.
`secglobalshow`	Admin	Displays current state information for Secure FOS, such as version stamp and status of transaction in progress.
`sechelp`	Admin	Displays a list of Secure Fabric OS commands. To use, enter the sechelp command at the CLI prompt.
`secmodedisable`	Admin	Disables Secure Mode.

Table 20: Secure Fabric OS Commands (Continued)

Command	Access Level	Description
secmodeenable	Admin	Enables Secure Mode. This command cannot be entered if Secure Mode is already enabled unless all the FCS switches have failed.
secmodeshow	Admin	Shows current mode of Secure Fabric OS.
secnonfcspasswd	Admin	Sets non-FCS admin account password.
secpolicyabort	Admin	Aborts all policy changes since changes were last saved.
secpolicyactivate	Admin	Activates all policy changes since this command was last issued All activated policy changes are stored in the active policy set.
secpolicyadd	Admin	Adds members to a policy.
secpolicycreate	Admin	Creates a policy.
secpolicydelete	Admin	Deletes a policy.
secpolicydump	Admin	Displays the Secure Fabric OS policy database.
secpolicyfcsmove	Admin	Moves an FCS member in the FCS list.
secpolicyremove	Admin	Removes members from a policy.
secpolicysave	Admin	Saves all policy changes since either secpolicysave or secpolicyactivate was last issued. All policy changes that are saved but not activated are stored in the defined policy set.
secpolicyshow	Admin	Shows members of one or more policies.
secstatsreset	Admin	Resets Secure Fabric OS statistics to 0.
secstatsshow	Admin	Displays Secure Fabric OS statistics.
sectemppasswdreset	Admin	Removes temporary passwords.
sectemppasswdset	Admin	Sets a temporary password for a switch.
sectransabort	Admin	Aborts the current Secure Fabric OS transaction.
secversionreset	Admin	Resets version stamp.

Command Restrictions in Secure Mode

This section provides information about the restrictions that Secure Mode places on commands. Any commands not listed here can be executed on any switch, whether or not Secure Mode is enabled.

Zoning Commands

All Zoning commands must be executed on the primary FCS switch, except for the `cfgshow` command which can also be executed on the backup FCS switch. Table 21 lists the Zoning commands.

Table 21: Zoning Commands

Command	Primary FCS Switch	Backup FCS Switch	Non-FCS Switch
`aliadd`	Yes	No	No
`alicreate`	Yes	No	No
`alidelete`	Yes	No	No
`aliremove`	Yes	No	No
`alishow`	Yes	No	No
`cfgadd`	Yes	No	No
`cfgclear`	Yes	No	No
`cfgcreate`	Yes	No	No
`cfgdelete`	Yes	No	No
`cfgdisable`	Yes	No	No
`cfgenable`	Yes	No	No
`cfgremove`	Yes	No	No
`cfgsave`	Yes	No	No
`cfgshow`	Yes	Yes	No
`cfgtransabort`	Yes	No	No
`cfgtransshow`	Yes	No	No
`fazoneadd`	Yes	No	No
`fazonecreate`	Yes	No	No

Command	Primary FCS Switch	Backup FCS Switch	Non-FCS Switch
fazonedelete	Yes	No	No
fazoneremove	Yes	No	No
fazoneshow	Yes	No	No
qloopadd	Yes	No	No
qloopcreate	Yes	No	No
qloopdelete	Yes	No	No
qloopremove	Yes	No	No
qloopshow	Yes	No	No
zoneadd	Yes	No	No
zonecreate	Yes	No	No
zonedelete	Yes	No	No
zoneremove	Yes	No	No
zoneshow	Yes	No	No

Miscellaneous Commands

Table 22 lists which miscellaneous commands, including Management Server and SNMP commands, can be executed on which switches. Commands not listed here (or in the preceding two tables) can be executed on any switch.

Table 22: Miscellaneous Commands

Command	Primary FCS Switch	Backup FCS Switch	Non-FCS Switch
agtcfgdefault	Yes	Yes, except cannot modify community strings	Yes, except cannot modify community strings
agtcfgset	Yes	Yes, except cannot modify community strings	Yes, except cannot modify community strings
cfgshow	Yes	Yes	No
cfgsize	Yes	Yes	Yes

Table 22: Miscellaneous Commands (Continued)

Command	Primary FCS Switch	Backup FCS Switch	Non-FCS Switch
`configupload`	Yes	Yes	Not recommended. The Zoning and Secure Fabric OS configurations are not uploaded if entered on a non-FCS switch.
`date`	Yes	Yes, but read only	Yes, but read only
`date <operand to set time>`	Yes	No	No
`mscapabilityshow`	Yes	Yes	Yes
`msconfigure`	Yes, except ACL does not display	Yes, except ACL does not display	Yes, except ACL does not display
`msplatshow`	Yes	Yes	Yes
`msplcleardb`	Yes	No	No
`msplmgmtactivate`	Yes	No	No
`msplmgmtdeactivate`	Yes	No	No
`mstddisable`	Yes	Yes	Yes
`mstddisable "all"`	Yes	No	No
`mstdenable`	Yes	Yes	Yes
`mstdenable "all"`	Yes	No	No
`mstdreadconfig`	Yes	Yes	Yes
`passwd`	Yes	No	No
`tsclockserver`	Yes	Yes	Yes
`tsclockserver <IP address of network time protocol (NTP) server>`	Yes	No	No
`wwn (display only; cannot modify WWNs in Secure Mode)`	Yes	Yes	Yes

Removing Secure Fabric OS Capability

B

Disabling Secure Mode includes the following steps:

- Preparing the Fabric for Removal of Secure Fabric OS Policies, page 145
- Disabling Secure Mode, page 146

In addition, the following steps can be taken if desired:

- Deactivating the Secure Fabric OS License on Each Switch, page 147
- Uninstalling Related Items from the Host, page 148

Overview

Secure Fabric OS capability can be removed from a fabric by disabling Secure Mode and deactivating the Secure Fabric OS license keys on the individual switches. Removing Secure Fabric OS capability is not recommended unless absolutely required. If at all possible, consider only disabling Secure Mode and leaving the Secure Fabric OS feature available so that Secure Mode can be re-enabled if desired.

One possible reason for disabling Secure Mode or removing Fabric OS capability includes the addition of new switches to the fabric that do not support Secure Fabric OS.

Preparing the Fabric for Removal of Secure Fabric OS Policies

Note: This section provides very general recommendations only.

HP recommends completing the following tasks to prepare the fabric before disabling Secure Mode:

- Review the current Secure Fabric OS policies and the devices and users affected by each policy. The current policy set can be displayed by entering the `secpolicydump` command.
- Review the types of attempted policy violations that have been occurring. The current Secure Fabric OS statistics can be displayed by entering the `secstatsshow` command.
- Evaluate the zoning configuration and other aspects of the fabric for any changes that could be implemented to decrease the chance of security violations when Secure Fabric OS is disabled.
- Educate users to minimize security risks and the impact of any security violations.

Disabling Secure Mode

Secure Mode is enabled and disabled on a fabric-wide basis and can be enabled and disabled as often as desired. However, all Secure Fabric OS policies, including the FCS policy, are deleted each time Secure Mode is disable, and must be re-created the next time it is enabled. The policies can be backed up using the `configupload` and `configdownload` commands. For more information about these commands, refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide*.

Secure Mode can be disabled only through a *sectelnet*, Secure Shell, or serial connection to the primary FCS switch. When Secure Mode is disabled, all current login sessions are automatically terminated.

For information about reenabling Secure Mode, see "Enabling Secure Mode" on page 66.

To disable Secure Mode, perform the following tasks:

1. From a *sectelnet*, Secure Shell, or serial session, log in to the primary FCS switch as admin.
2. Type `secmodedisable`.
3. Type the password when prompted.
4. Type **y** to verify that Secure Mode should be disabled.

   Secure Mode is disabled, all *current login* sessions are terminated, and the passwords are modified as follows:

   — On the switches that were FCS switches, the user, admin, factory, and root passwords remain the same as in Secure Mode.

   — On the switches that were non-FCS switches, the root, factory, and admin passwords become the same as the non-FCS admin password.

Example

```
primaryfcs:admin> secmodedisable
Warning!!!
About to disable security.
ARE YOU SURE (yes, y, no, n): [no] y
Committing configuration...done.
Removing Active FMPS...
done
Removing Defined FMPS...
done
Disconnecting current session.
primaryfcs:admin>
```

Deactivating the Secure Fabric OS License on Each Switch

Deactivating the Secure Fabric OS license is not required to disable Secure Fabric OS functionality.

Note: If the user installs and activates a feature license and then removes the license, the feature is not disabled until the next time system is rebooted or a switch enable/disable is performed.

To deactivate the software license:

1. Open a CLI connection (serial or telnet) to the switch.
2. Type the `licenseidshow` command to display the Secure Fabric OS license key.
3. Type the following:

   `licenseremove` "*key*"

   key is the license key and is case sensitive. It can be copied from the `licenseshow` output directly into the CLI.
4. Repeat for each switch in the fabric.

Example

```
switch:admin> licenseremove "1A1AaAaaaAAAA1a"
removing license-key "1A1AaAaaaAAAA1a"
Committing configuration...done.
For license to take effect, Please reboot switch now....
switch:admin>
```

Uninstalling Related Items from the Host

The following items can optionally be removed from the host:

- PKICERT utility
- `sectelnet`
- Secure Shell client

These items do not have to be uninstalled to disable Secure Fabric OS functionality.

Follow the standard procedure for uninstalling software from the workstation. On a Windows host computer, use the `Add/Remove Programs` control panel or just delete the folder. On a Solaris host, use the `rm` command to remove the folder.

glossary

This glossary defines terms used in this guide or related to this product and is not a comprehensive glossary of computer terms.

A

AL_PA
Arbitrated loop physical address. A unique 8-bit value assigned during loop initialization to a port in an arbitrated loop.

alias server
A fabric software facility that supports multicast group management.

API
Application programming interface. A defined protocol that allows applications to interface with a set of services.

AW_TOV
Arbitration wait time-out value. The minimum time an arbitrating L_Port waits for a response before beginning loop initialization.

B

backup FCS switch
Backup fabric configuration server switch. The switch or switches assigned as backup in case the primary FCS switch fails.

bandwidth
The total transmission capacity of a cable, link, or system. Usually measured in bps (bits per second). May also refer to the range of transmission frequencies available to a link or system.

broadcast
The transmission of data from a single source to all devices in the fabric, regardless of zoning.

buffer-to-buffer flow control
Management of the frame transmission rate in either a point-to-point topology or in an arbitrated loop.

C

CLI
Command line interface. Interface that depends entirely on the use of commands, such as through telnet or SNMP, and does not involve a GUI.

compact flash
Flash (temporary) memory that is used in a manner similar to hard disk storage. It is connected to a bridging component which connects to the PCI bus of the processor. Not visible within the processor's memory space.

Configuration
The way in which a system is set up. May refer to hardware or software.

CRC
Cyclic redundancy check. A check for transmission errors that is included in every data frame.

D

data word
A type of transmission word that occurs within frames. The frame header, data field, and CRC all consist of data words.

defined zone configuration
The set of all zone objects defined in the fabric. May include multiple zone configurations.

DLS
Dynamic load sharing. Dynamic distribution of traffic over available paths. Allows for recomputing of routes when an Fx_Port or E_Port changes status.

domain ID
Unique identifier for all switches in a fabric, used in routing frames. Usually automatically assigned by the principal switch, but can be assigned manually. The domain ID for an HP StorageWorks switch can be any integer between 1 and 239. Generally, the default domain ID is 1.

E

E_D_TOV
Error detect time-out value. The minimum amount of time a target waits for a sequence to complete before initiating recovery. Can also be defined as the maximum time allowed for a round-trip transmission before an error condition is declared.

E_Port
Expansion port. A type of switch port that can be connected to an E_Port on another switch to create an ISL.

EE_Credit
End-to-end credit. The number of receive buffers allocated by a recipient port to an originating port. Used by Class 1 and 2 services to manage the exchange of frames across the fabric between source and destination.

EIA rack
A storage rack that meets the standards set by the Electronics Industry Association.

enabled zone configuration
The currently enabled configuration of zones. Only one configuration can be enabled at a time.

end-to-end flow control
Governs flow of class 1 and 2 frames between N_Ports.

error
As applies to fibre channel, a missing or corrupted frame, time-out, loss of synchronization, or loss of signal (link errors).

exchange
The highest level fibre channel mechanism used for communication between N_Ports. Composed of one or more related sequences, and can work in either one or both directions.

F

F_Port
Fabric port. A port that is able to transmit under fabric protocol and interface over links. Can be used to connect an N_Port to a switch.

fabric
A fibre channel network containing two or more switches in addition to hosts and devices. May also be referred to as a switched fabric.

fabric name
The unique identifier assigned to a fabric and communicated during login and port discovery.

FCIA
Fibre Channel Industry Association. An international organization of fibre channel industry professionals. Among other things, provides oversight of ANSI and industry developed standards.

FCP
Fibre channel protocol. Mapping of protocols onto the fibre channel standard protocols. For example, SCSI FCP maps SCSI-3 onto fibre channel.

FCS switch
Fabric Configuration Server Switch. One or more designated switches that store and manage the configuration and security parameters for all switches in the fabric. FCS switches are designated by WWN, and the list of designated switches is communicated fabric-wide.

fill word
An IDLE or ARB ordered set that is transmitted during breaks between data frames to keep the fibre channel link active.

FL_Port
Fabric loop port. A port that is able to transmit under fabric protocol and also has arbitrated loop capabilities. Can be used to connect an NL_Port to a switch.

FRU
Field-Replaceable Unit. A component that can be replaced on site.

FS
Fibre Channel Service. A service that is defined by fibre channel standards and exists at a well-known address. For example, the Simple Name Server is a fibre channel service.

FSP
Fibre channel service protocol. The common protocol for all fabric services, transparent to the fabric type or topology.

FSPF
Fabric shortest path first. The routing protocol used by HP for fibre channel switches.

Fx_Port
A fabric port that can operate as either an F_Port or FL_Port.

G

G_Port
Generic port. A port that can operate as either an E_Port or F_Port. A port is defined as a G_Port when it is not yet connected or has not yet assumed a specific function in the fabric.

H

hard address
The AL_PA that an NL_Port attempts to acquire during loop initialization.

I

idle
Continuous transmission of an ordered set over a fibre channel link when no data is being transmitted, to keep the link active and maintain bit, byte, and word synchronization.

integrated fabric
The fabric created by connecting multiple HP StorageWorks switches with multiple ISL cables, and configuring the switches to handle traffic as a seamless group.

ISL trunking
The distribution of traffic over the combined bandwidth of multiple ISLs. A set of trunked ISLs is called a “trunking group”, and the ports in a trunking group are called “trunking ports”.

isolated E_Port
An E_Port that is online but not operational due to overlapping domain IDs or nonidentical parameters (such as E_D_TOVs).

K

K28.5
A special 10-bit character used to indicate the beginning of a transmission word that performs fibre channel control and signaling functions. The first seven bits of the character are the comma pattern.

kernel flash
Flash (temporary) memory connected to the peripheral bus of the processor, and visible within the processor's memory space. Also known as “user flash”.

L

L_Port
Loop port. A node port (NL_Port) or fabric port (FL_Port) that has arbitrated loop capabilities. An L_Port can be in one of two modes:

latency
The period of time required to transmit a frame, from the time it is sent until it arrives. Together, latency and bandwidth define the speed and capacity of a link or system.

link
As applies to fibre channel, a physical connection between two ports, consisting of both transmit and receive fibers.

link services
A protocol for link-related actions.

LIP
Loop initialization primitive. The signal used to begin initialization in a loop. Indicates either loop failure or resetting of a node.

LM_TOV
Loop master time-out value. The minimum time that the loop master waits for a loop initialization sequence to return.

loop failure
Loss of signal within a loop for any period of time, or loss of synchronization for longer than the time-out value.

loop initialization
The logical procedure used by an L_Port to discover its environment. Can be used to assign AL_PA addresses, detect loop failure, or reset a node.

Loop_ID
A hex value representing one of the 127 possible AL_PA values in an arbitrated loop.

LPSM
Loop port state machine. The logical entity that performs arbitrated loop protocols and defines the behavior of L_Ports when they require access to an arbitrated loop.

LWL
Long wavelength. A type of fiber optic cabling that is based on 1300 mm lasers and supports link speeds up to 2 Gb/s May also refer to the type of transceiver.

M

master port
The port that determines the routing paths for all traffic flowing through a trunking group. One of the ports that is in the first ISL in the trunking group is designated as the master port for that group.

MIB
Management Information Base. An SNMP structure to help with device management, providing configuration and device information.

multicast
The transmission of data from a single source to multiple specified N_Ports (as opposed to all the ports on the network).

N

N_Port
Node port. A port on a node that can connect to a fibre channel port or to another port in a point-to-point connection.

name server
Frequently used to indicate Simple Name Server.

NL_Port
Node loop port. A node port that has arbitrated loop capabilities. Used to connect an equipment port to the fabric in a loop configuration through an FL_Port.

node
A fibre channel device that contains an N_Port or NL_Port.

non-participating mode
A mode in which an L_Port in a loop is inactive and cannot arbitrate or send frames, but can retransmit any received transmissions. This mode is entered if there are more than 127 devices in a loop and an AL_PA cannot be acquired.

Nx_Port
A node port that can operate as either an N_Port or NL_Port.

P

packet
A set of information transmitted across a network.

participating mode
A mode in which an L_Port in a loop has a valid AL_PA and can arbitrate, send frames, and retransmit received transmissions.

path selection
The selection of a transmission path through the fabric. HP switches use the FSPF protocol.

phantom address
An AL_PA value that is assigned to an device that is not physically in the loop. Also known as phantom AL_PA.

phantom device
A device that is not physically in an arbitrated loop but is logically included through the use of a phantom address.

PLOGI
Port login. The port-to-port login process by which initiators establish sessions with targets.

point-to-point
A fibre channel topology that employs direct links between each pair of communicating entities.

port cage
The metal casing extending out of the fibre channel port on the switch, and into which a GBIC or SFP transceiver can be inserted.

Port_Name
The unique identifier assigned to a fibre channel port. Communicated during login and port discovery.

POST
Power On Self-Test. A series of tests run by a switch after it is powered on.

primary FCS switch
Primary fabric configuration server switch. The switch that actively manages the configuration and security parameters for all switches in the fabric.

private loop
An arbitrated loop that does not include a participating FL_Port.

private NL_Port
An NL_Port that communicates only with other private NL_Ports in the same loop and does not log into the fabric.

public device
A device that supports arbitrated loop protocol, can interpret 8-bit addresses, and can log into the fabric.

public loop
An arbitrated loop that includes a participating FL_Port, and may contain both public and private NL_Ports.

public NL_Port
An NL_Port that logs into the fabric, can function within either a public or a private loop, and can communicate with either private or public NL_Ports.

Q

quad
A group of four adjacent ports that share a common pool of frame buffers.

R

R_A_TOV
Resource allocation time-out value. The maximum time a frame can be delayed in the fabric and still be delivered.

RAID
Redundant Array Of Independent Disks. A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking.

request rate
The rate at which requests arrive at a servicing entity.

route
As applies to a fabric, the communication path between two switches. May also apply to the specific path taken by an individual frame, from source to destination.

routing
The assignment of frames to specific switch ports, according to frame destination.

RR_TOV
Resource recovery time-out value. The minimum time a target device in a loop waits after a LIP before logging out a SCSI initiator.

RSCN
Registered state change notification. A switch function that allows notification of fabric changes to be sent from the switch to specified nodes.

S

SAN
Storage Area Network. A network of systems and storage devices that communicate using fibre channel protocols.

SDRAM
The main memory for the switch.

sequence
A group of related frames transmitted in the same direction between two N_Ports.

service rate
The rate at which an entity can service requests.

single mode
The fiber optic cabling standard that corresponds to distances of up to 10 km between devices.

SNMP
Simple Network Management Protocol. An Internet management protocol that uses either IP for network-level functions and UDP for transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols.

SNS
Simple Name Server. A switch service that stores names, addresses, and attributes for up to 15 minutes, and provides them as required to other devices in the fabric. SNS is defined by fibre channel standards and exists at a well-known address. May also be referred to as directory service.

switch
Hardware that routes frames according to fibre channel protocol and is controlled by software.

switch port
A port on a switch. Switch ports can be E_Ports, F_Ports, or FL_Ports.

SWL
Short wavelength. A type of fiber optic cabling that is based on 850 mm lasers and supports link speeds up to 2 Gb/s May also refer to the type of transceiver.

T

tenancy
The time from when a port wins arbitration in a loop until the same port returns to the monitoring state. Also referred to as loop tenancy.

throughput
The rate of data flow achieved within a cable, link, or system. Usually measured in bps (bits per second).

topology
As applies to fibre channel, the configuration of the fibre channel network and the resulting communication paths allowed. There are three possible topologies:

- **Point to point**: A direct link between two communication ports.
- **Switched fabric**: Multiple N_Ports linked to a switch by F_Ports.
- **Arbitrated loop**: Multiple NL_Ports connected in a loop.

transmission character
A 10-bit character encoded according to the rules of the 8b/10b algorithm.

transmission word
A group of four transmission characters.

trap (SNMP) The message sent by an SNMP agent to inform the SNMP management station of a critical error.

U

U_Port
Universal port. A switch port that can operate as a G_Port, E_Port, F_Port, or FL_Port. A port is defined as a U_Port when it is not connected or has not yet assumed a specific function in the fabric.

W

well-known address
As pertaining to fibre channel, a logical address defined by the fibre channel standards as assigned to a specific function, and stored on the switch.

workstation
A computer used to access and manage the fabric. May also be referred to as a management station or host.

WWN
World Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

Z

zone
A set of devices and hosts attached to the same fabric and configured as being in the same zone. Devices and hosts within the same zone have access permission to others in the zone, but are not visible to any outside the zone.

zone configuration
A specified set of zones. Enabling a configuration enables all zones in that configuration.

index

T

U

V

W